

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001年3月8日 (08.03.2001)

PCT

(10) 国際公開番号  
WO 01/16776 A1

(51) 国際特許分類:  
17/60, H04L 9/08, G10K 15/02

G06F 15/00,

(72) 発明者; および

(75) 発明者/出願人 (米国についてののみ): 石橋義人 (ISHIBASHI, Yoshihito) [JP/JP]. 大石文於 (OHISHI, Tateo) [JP/JP]. 松山科子 (MATSUYAMA, Shinako) [JP/JP]. 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 武藤明宏 (MUTO, Akihiro) [JP/JP]. 北原 淳 (KITAHARA, Jun) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(21) 国際出願番号:

PCT/JP00/05742

(22) 国際出願日:

2000年8月25日 (25.08.2000)

(25) 国際出願の言語:

日本語

(26) 国際公開の言語:

日本語

(30) 優先権データ:

特願平11/242294	1999年8月27日 (27.08.1999)	JP
特願平11/242295	1999年8月27日 (27.08.1999)	JP
特願平11/242296	1999年8月27日 (27.08.1999)	JP
特願平11/283326	1999年8月27日 (27.08.1999)	JP

(74) 代理人: 弁理士 田辺恵基 (TANABE, Shigemoto); 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンファンタジアビル5階 Tokyo (JP).

(81) 指定国 (国内): CN, KR, US.

(84) 指定国 (広域): ヨーロッパ特許 (DE, FR, GB).

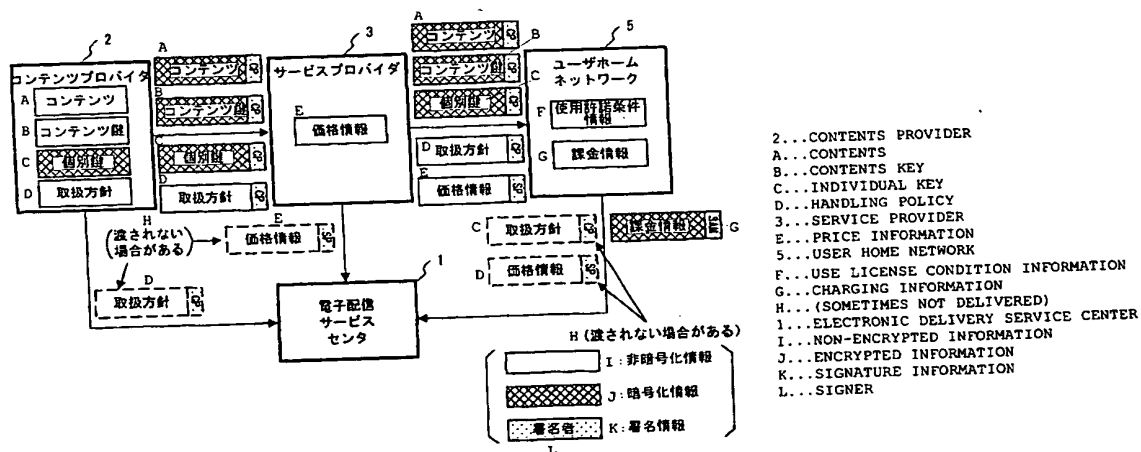
(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

添付公開書類:  
— 国際調査報告書

[続葉有]

(54) Title: INFORMATION TRANSMISSION SYSTEM, TRANSMITTER, AND TRANSMISSION METHOD AS WELL AS INFORMATION RECEPTION SYSTEM, RECEIVER AND RECEPTION METHOD

(54) 発明の名称: 情報送信システム、装置及び方法並びに情報受信システム、装置及び方法



(57) Abstract: An information transmitter transmits to an information receiver contents data encrypted with a contents key, a contents key encrypted with an individual key specific to the information transmitter, and the individual key encrypted by a delivery key, the contents key encrypted with an individual key specific to the information transmitter, and the individual key encrypted by a delivery key, the contents key with the individual key, and the contents data with the contents key. Since the information transmitter has no delivery key, the contents data is not stolen. The information receiver transmits the contents key and a reproduction command to another device, which reproduces the contents with the contents key according to the reproduction command. The information transmitter decodes the contents key with the individual key decoded with the delivery key before update and stores it. Therefore, irrespective of the valid term of the delivery key, the user can purchase the subscribed contents. An information receiver having registered information in using the contents can transfer the right of use to another information receiver having different registered information so as to use the contents.

[続葉有]

WO 01/16776 A1



— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

コンテンツ鍵で暗号化したコンテンツデータと、情報送信装置固有の個別鍵で暗号化したコンテンツ鍵と、所定周期で更新される配送鍵で暗号化して供給された個別鍵とを情報受信装置に送信し、情報受信装置が配送鍵で個別鍵を復号し、当該個別鍵でコンテンツ鍵を復号し、当該コンテンツ鍵でコンテンツデータを復号する。従って情報送信装置が配送鍵を持たない分、簡易な構成でコンテンツデータの盗用を防止できる。また、情報受信装置はコンテンツ鍵と再生コマンドとを他の機器に送信する。従って他の機器は再生コマンド及びコンテンツ鍵を用いてコンテンツを再生できる。さらに、情報送信装置は更新前の配送鍵で復号した個別鍵でコンテンツ鍵を復号して保存する。従って配送鍵の有効期限に係わらずに予約購入したコンテンツを本購入できる。さらに、コンテンツ利用時の登録情報が異なる第1の情報受信装置から第2の情報受信装置に利用権を引き渡す。従って登録情報が異なる情報受信装置間でコンテンツを利用可能にできる。

## 明 細 書

情報送信システム、装置及び方法並びに情報受信システム、装置及び方法

## 技術分野

本発明は情報送信システム、情報送信装置、情報受信装置、情報配信システム、情報受信システム、情報送信方法、情報受信方法、情報配信方法、機器、情報受信装置の送信方法、機器の再生方法、コンテンツの利用方法およびプログラム格納媒体に関し、例えばコンテンツ保有者又は販売者が、コンテンツを安全にコンテンツ利用者に配送し得る情報送信システムに適用して好適なものである。

## 背景技術

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザがその情報処理装置でコンテンツを復号して、利用するシステムがある。

例えば図 9 6 に示すように、2つのコンテンツ送信装置および1つのコンテンツ受信装置が設けられている場合について説明する。

第1のコンテンツ送信装置 600 は、データ暗号部 601、データ暗号部 602、コンテンツ鍵生成部 603、耐タンパメモリ (Tamper Resistant Memory) 604 を有している。なお、ここで言う耐タンパメモリとは、第3者に容易にデータを読み出されないものであればよく、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。耐タンパメモリ 604 にはコンテンツ鍵 (Content Key)  $K_c$  を暗号化するのに必要な配送鍵 (Distribution Key)  $K_d$  が、予め電子配

信サービスセンタ（図示せず）から供給され、保存されている。

コンテンツ送信装置 600 は、コンテンツ受信装置 620 に渡すデータを生成するため、コンテンツ鍵生成部 603 を用いてコンテンツ鍵  $K_{co1}$  を生成し、この鍵を用いてデータ暗号部 601 にてコンテンツを暗号化する。また、コンテンツ鍵  $K_{co1}$  はデータ暗号部 602 にて配送鍵  $K_d$  を用いて暗号化される。これら暗号化されたコンテンツおよびコンテンツ鍵  $K_{co1}$  がコンテンツ受信装置 620 に送信される。

因に、第 2 のコンテンツ送信装置 610 は、コンテンツ送信装置 600 と同様にして、データ暗号部 611、データ暗号部 612、コンテンツ鍵生成部 613、耐タンパメモリ 614 を有し、コンテンツ鍵生成部 613 においてコンテンツ鍵  $K_{co2}$  を生成し、この鍵を用いてデータ暗号部 611 によりコンテンツを暗号化する。またデータ暗号部 612 は電子配信サービスセンタ（図示せず）から供給される配送鍵  $K_d$  を用いてコンテンツ鍵  $K_{co2}$  を暗号化する。かくして第 2 のコンテンツ送信装置 610 は、暗号化されたコンテンツ及び暗号化されたコンテンツ鍵  $K_{co2}$  をコンテンツ受信装置 620 に送信する。

コンテンツ受信装置 620 は、送受信部 621、上位コントローラ 622、暗号処理部 623、メモリ 624、データ復号部 625、データ復号部 626、耐タンパメモリ 627 を有する。なお、コンテンツ利用者が不特定多数であり、コンテンツ利用者が機器をどのように扱うか把握できないため、ここで言う耐タンパメモリとはハードウェア的に内部データが保護される必要性があり、従って暗号処理部 623 は、外部からアクセスしにくい構造を持った半導体チップで、多層構造を有し、その内部の耐タンパメモリはアルミニウム層等のダミー層に挟まれ、また、動作する電圧及び又は周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する。そして、耐タンパメモリ 627 には、電子配信サービスセンタ（図示せず）から予め供給された配送鍵  $K_d$  が保存されている。

因に、コンテンツ送信装置 600 及び 610 の耐タンパメモリ 604、614



は、外部からアクセス可能なメモリであるが、そのアクセス方法に制約を設けている。それがパスワードであったり、入室管理であったりする。一方、コンテンツ受信装置 620 の耐タンパメモリ 627 においては、メモリそのものが外部から不正にアクセスされない構造を有し、正規のアクセス手段で外部から内部データを読み出す方法も限定されているか、全くない。なお、耐タンパメモリ 627 は外部からその内部データを読み出すことは全くできないが、以前の鍵データ等を用いれば、外部からデータの変更のみできるアクセス方法がある場合がある。また、暗号処理部 623 内では、メモリにアクセスして所定のデータを読み出すことができるのに対して、外部から内部のメモリを読み出すことができないようになされている。

コンテンツ送信者 600 または 610 から送信されてきたコンテンツおよびコンテンツ鍵  $K_{\infty 1}$  及び  $K_{\infty 2}$  は、送受信部 621 で受信され、上位コントローラ 622 に引き渡される。上位コントローラ 622 は、これらのデータをいったんメモリ 624 に保存し、コンテンツを利用する場合には、コンテンツ鍵  $K_{\infty}$ 、コンテンツを暗号処理部 623 に引き渡す。これを受信した暗号処理部 623 は、データ復号部 625 で予め耐タンパメモリ 627 に保存しておいた配送鍵  $K_d$  を用いて復号化し、引き続きコンテンツをデータ復号部 626 でコンテンツ鍵  $K_{\infty}$  を用いて復号化し、コンテンツを利用する。この時、課金処理を伴う場合がある。

しかしながら、図 96 に示す従来の情報処理システムにおいては、コンテンツ送信装置 600 および 610 が同一の配送鍵  $K_d$  を使用しているため、互いにコンテンツ情報を盗み取ることができる問題があった。この問題点を解決するための一つの方法として、コンテンツ送信装置毎に異なる配送鍵  $K_d$  を使用することにより送信装置相互のコンテンツ情報の盗用を防止する方法が考えられる。ところが、この場合、コンテンツ受信装置が全ての配送鍵  $K_d$  を保持しておく必要があり、この分受信装置の構成及び受信方法が煩雑になる問題があった。

また、コンテンツを受信する情報受信装置のうち、コンテンツの利用権を有していない情報受信装置ではコンテンツを利用することが困難であった。

さらに、情報送信装置から配信される配送鍵 $K_d$ やその他コンテンツを利用するために必要とされる情報は所定のタイミングで更新されており、新しい配送鍵 $K_d$ やその他の情報を持っていない情報受信装置はコンテンツを利用することが困難であった。

さらに、コンテンツを利用する複数の情報受信装置において、コンテンツを利用するための登録情報が異なる場合には、当該登録情報が異なる情報受信装置間ではコンテンツデータの授受を行うことが困難であった。

#### 発明の開示

本発明は以上の点を考慮してなされたもので、簡易な構成でコンテンツの盗用を防止し得る情報送信システム、情報配信システム、情報送信装置、情報受信装置、情報送信方法、情報受信方法およびプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報送信装置は、コンテンツデータを所定のコンテンツ鍵で暗号化すると共に、情報送信装置固有の個別鍵で上記コンテンツ鍵を暗号化し、コンテンツ鍵で暗号化されたコンテンツデータと、個別鍵で暗号化されたコンテンツ鍵と、所定の配送鍵で個別鍵を暗号化してなる外部から供給された暗号化個別鍵とを情報受信装置に送信し、情報受信装置は、予め与えられている配送鍵で個別鍵を復号し、当該復号された個別鍵でコンテンツ鍵を復号し、当該復号されたコンテンツ鍵でコンテンツデータを復号するようにした。

従って、複数の情報送信装置は、それぞれ固有の個別鍵を使用して配送鍵を持たないことにより、情報送信装置間のコンテンツデータの不正使用、すなわち盗用を防止することができる。そして情報受信装置は、1種類の配送鍵を持つだけで複数の情報送信装置からのコンテンツを復号することができる。

また、本発明は以上の点を考慮してなされたもので、コンテンツを利用する情報受信装置のうち、コンテンツの利用権を有していない情報受信装置でもコンテ

ンツを利用できる情報配信システム、情報配信方法、情報受信装置、機器、情報受信装置の送信方法、機器の再生方法およびプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、コンテンツの利用権を有する情報受信装置は、情報送信装置から配信されるコンテンツデータを復号するためのコンテンツ鍵を有し、コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成し、当該生成された再生コマンド及びコンテンツ鍵を他の機器に送信するようにした。

従って、コンテンツを再生する権利を保持していない他の機器においても、コンテンツを保持している情報送信装置から受け取った再生コマンド及びコンテンツ鍵を用いてコンテンツを再生することができる。

さらに、本発明は以上の点を考慮してなされたもので、情報送信装置から配信される配送鍵やその他コンテンツを利用するために必要とされる情報の有効期限が切れてもコンテンツを利用し得る情報配信システム、情報配信方法、情報受信装置、情報受信方法およびプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、情報送信装置は、情報送信装置固有の個別鍵でコンテンツ鍵を暗号化し、少なくとも個別鍵で暗号化されたコンテンツ鍵と、所定の周期で更新される配送鍵で個別鍵を暗号化してなる外部から供給された暗号化個別鍵とを情報受信装置に送信し、情報受信装置は、配送鍵が更新される前に、予め与えられている配送鍵で個別鍵を復号し、当該復号された個別鍵でコンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存するようにした。

従って、情報受信装置は、配送鍵の有効期限が切れる前に購入予約によるコンテンツ鍵の復号を行っておくことにより、当該配送鍵が更新された後にコンテンツを復号することができ、かくして、配送鍵の有効期限が切れた後でも予約購入しているコンテンツを本購入することができる。

さらに、本発明は以上の点を考慮してなされたもので、コンテンツを利用する

ための登録情報が異なる受信装置間でコンテンツデータの授受を可能とする情報受信システム、コンテンツの利用方法およびプログラム格納媒体を提案しようとするものである。

かかる課題を解決するため本発明においては、コンテンツデータを利用するための登録情報が異なる複数の情報受信装置間で登録情報を授受することにより複数の情報受信装置間でコンテンツデータの利用可否を相互に判断し、複数の情報受信装置のうちコンテンツデータの利用権を有する第1の情報受信装置がコンテンツデータの利用可と判断した第2の情報受信装置に対して利用権を引き渡すようにした。

従って、コンテンツデータを利用するための登録情報が異なるグループ間において、第1の情報受信装置から利用権が引き渡された第2の情報受信装置でコンテンツを利用可能として、互いに登録情報が異なる情報受信装置間でもコンテンツデータの授受を行うことができ、かくして、ユーザの使い勝手を一段と向上することができる。

#### 図面の簡単な説明

図1は、本発明による電子音楽配信システムの全体構成を示すブロック図である。

図2は、電子配信サービスセンタの構成を示すブロック図である。

図3は、鍵の定期的な更新例を示す略線図である。

図4は、鍵の定期的な更新例を示す略線図である。

図5は、鍵の定期的な更新例を示す略線図である。

図6は、鍵の定期的な更新例を示す略線図である。

図7は、ユーザ登録データベースのデータ内容を示す略線図である。

図8は、グループごとの登録情報を示す略線図である。

図9は、コンテンツプロバイダの構成を示すブロック図である。

図10は、署名生成処理手順を示すフローチャートである。

- 図 1 1 は、署名検証処理手順を示すフローチャートである。
- 図 1 2 は、楕円曲線暗号化方法を示すフローチャートである。
- 図 1 3 は、楕円曲線暗号化の復号化処理を示すフローチャートである。
- 図 1 4 は、サービスプロバイダの構成を示すブロック図である。
- 図 1 5 は、ユーザホームネットワークの構成を示すブロック図である。
- 図 1 6 は、外部メモリ制御部の動作の説明に供する略線図である。
- 図 1 7 は、電子配信専用記録メディアの構成を示すブロック図である。
- 図 1 8 は、各機器の持つデータ内容を示すブロック図である。
- 図 1 9 は、記録メディアが保持するデータ内容を示すブロック図である。
- 図 2 0 は、システム全体のデータの流れを示す略線的ブロック図である。
- 図 2 1 は、公開鍵証明書の流れを示す略線的ブロック図である。
- 図 2 2 は、コンテンツプロバイダセキュアコンテナを示す略線図である。
- 図 2 3 は、コンテンツプロバイダセキュアコンテナを示す略線図である。
- 図 2 4 は、コンテンツプロバイダセキュアコンテナを示す略線図である。
- 図 2 5 は、コンテンツプロバイダセキュアコンテナを示す略線図である。
- 図 2 6 は、コンテンツプロバイダの公開鍵証明書を示す略線図である。
- 図 2 7 は、コンテンツプロバイダの公開鍵証明書を示す略線図である。
- 図 2 8 は、コンテンツプロバイダの公開鍵証明書を示す略線図である。
- 図 2 9 は、サービスプロバイダセキュアコンテナを示す略線図である。
- 図 3 0 は、サービスプロバイダセキュアコンテナを示す略線図である。
- 図 3 1 は、サービスプロバイダの公開鍵証明書を示す略線図である。
- 図 3 2 は、ユーザ機器の公開鍵証明書を示す略線図である。
- 図 3 3 は、シングルコンテンツの取扱方針を示す略線図である。
- 図 3 4 は、アルバムコンテンツの取扱方針を示す略線図である。
- 図 3 5 は、シングルコンテンツの取扱方針の他の例を示す略線図である。
- 図 3 6 は、アルバムコンテンツの取扱方針の他の例を示す略線図である。
- 図 3 7 は、シングルコンテンツの価格情報を示す略線図である。

- 図 3 8 は、アルバムコンテンツの価格情報を示す略線図である。
- 図 3 9 は、シングルコンテンツの価格情報の他の例を示す略線図である。
- 図 4 0 は、アルバムコンテンツの価格情報の他の例を示す略線図である。
- 図 4 1 は、使用許諾条件情報を示す略線図である。
- 図 4 2 は、課金情報を示す略線図である。
- 図 4 3 は、課金情報の他の例を示す略線図である。
- 図 4 4 は、利用権内容の一覧を示す略線図である。
- 図 4 5 は、利用権を示す略線図である。
- 図 4 6 は、シングルコンテンツを示す略線図である。
- 図 4 7 は、アルバムコンテンツを示す略線図である。
- 図 4 8 は、シングルコンテンツ用の鍵データを示す略線図である。
- 図 4 9 は、個別鍵の暗号化処理の説明に供するブロック図である。
- 図 5 0 は、アルバムコンテンツ用の鍵データを示す略線図である。
- 図 5 1 は、対称鍵技術を用いた相互認証処理を示すタイミングチャートである。
- 図 5 2 は、非対称鍵暗号技術を用いた相互認証処理を示すタイミングチャートである。
- 図 5 3 は、課金情報の送信動作を示す略線的ブロック図である。
- 図 5 4 は、利益分配処理動作を示す略線的ブロック図である。
- 図 5 5 は、コンテンツ利用実績の送信動作を示す略線的ブロック図である。
- 図 5 6 は、コンテンツの配布及び再生処理手順を示すフローチャートである。
- 図 5 7 は、コンテンツプロバイダへの送信処理手順を示すフローチャートである。
- 図 5 8 は、決済情報の登録処理手順を示すフローチャートである。
- 図 5 9 は、機器 I D の新規登録処理手順を示すフローチャートである。
- 図 6 0 は、機器の追加登録処理手順を示すフローチャートである。
- 図 6 1 は、登録情報の更新開始条件の判断処理を示すフローチャートである。

図 6 2 は、登録情報更新処理手順を示すフローチャートである。

図 6 3 は、据置機器による登録情報更新代理処理手順を示すフローチャートである。

図 6 4 は、据置機器による登録情報更新代理処理手順を示すフローチャートである。

図 6 5 は、セキュアコンテナの送信処理手順を示すフローチャートである。

図 6 6 は、セキュアコンテナの送信処理手順を示すフローチャートである。

図 6 7 は、ホームサーバの購入処理手順を示すフローチャートである。

図 6 8 は、データ読み出し時の改竄チェック処理手順を示すフローチャートである。

図 6 9 は、データ書込み時の改竄チェック処理手順を示すフローチャートである。

図 7 0 は、データ書換え時の改竄チェック処理手順を示すフローチャートである。

図 7 1 は、データ削除時の改竄チェック処理手順を示すフローチャートである。

図 7 2 は、ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

図 7 3 は、ホームサーバによるコンテンツの再生処理手順を示すフローチャートである。

図 7 4 は、ホームサーバによるコンテンツ利用権の代理購入処理手順を示すフローチャートである。

図 7 5 は、購入済利用者の内容変更処理手順を示すフローチャートである。

図 7 6 は、取扱方針のルール部の内容を示す略線図である。

図 7 7 は、価格情報のルール部の内容を示す略線図である。

図 7 8 は、権利内容の変更例を示す略線図である。

図 7 9 は、コンテンツ利用権の再配布処理手順を示すフローチャートである。

図 8 0 は、据置機器でのコンテンツ利用権購入処理手順を示すフローチャートである。

図 8 1 は、使用許諾条件情報のルール部の変遷を示す略線図である。

図 8 2 は、管理移動権の移動処理手順を示すフローチャートである。

図 8 3 は、管理移動権の返還処理手順を示すフローチャートである。

図 8 4 は、本発明による情報送信システムを示すブロック図である。

図 8 5 は、本発明による情報送信システムを示すブロック図である。

図 8 6 は、遠隔再生処理手順を示すフローチャートである。

図 8 7 は、予約購入処理手順を示すフローチャートである。

図 8 8 は、予約購入後の本購入処理手順を示すフローチャートである。

図 8 9 は、ホームサーバが課金する場合の代理購入処理手順を示すフローチャートである。

図 9 0 は、グループ外機器が課金する場合の代理購入処理手順を示すフローチャートである。

図 9 1 は、電子音楽配信システムの他の構成を示すブロック図である。

図 9 2 は、パーソナルコンピュータ構成の電子配信サービスセンターの構成を示すブロック図である。

図 9 3 は、パーソナルコンピュータ構成のコンテンツプロバイダの構成を示すブロック図である。

図 9 4 は、パーソナルコンピュータ構成のサービスプロバイダの構成を示すブロック図である。

図 9 5 は、パーソナルコンピュータを用いたユーザホームネットワークの構成を示すブロック図である。

図 9 6 は、従来例を示すブロック図である。

発明を実施するための最良の形態

以下、図面について本発明の一実施の形態を詳述する。



### (1) 情報配信システム

図1は、本発明を適用したEMD (Electronic Music Distribution: 電子音楽配信) システム10を説明する図である。このシステムでユーザに配信されるコンテンツ (Content) とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。コンテンツは、1つのコンテンツが1つの単位 (シングル) として、または複数のコンテンツが1つの単位 (アルバム) としてユーザに提供される。ユーザは、コンテンツを購入し (実際には、コンテンツ鍵 $K_c$ を利用する権利を購入し)、提供されるコンテンツを利用する (実際には、コンテンツ鍵 $K_c$ を用いてコンテンツを復号化し、利用する)。なお、勿論、音楽データだけでなく、映像、ゲームプログラム等、コンテンツの販売全てに適用可能である。

電子配信サービスセンタ (END Service Center) 1は、コンテンツプロバイダ (Content Provider) 2に個別鍵 $K_i$ 、コンテンツプロバイダ2の公開鍵証明書を送信し、サービスプロバイダ (Service Provider) 3にサービスプロバイダ3の公開鍵証明書を送信し、ユーザホームネットワーク5に対しては配送鍵 $K_d$ や登録情報を送信し、ユーザホームネットワーク5から、コンテンツの利用に応じた課金情報等や登録情報を受信し、課金情報に基づいて利用料金を精算し、コンテンツプロバイダ2、サービスプロバイダ3および電子配信サービスセンタ1自身へ利益分配の処理を行う。

コンテンツプロバイダ2は、デジタル化されたコンテンツを有し、自己のコンテンツであることを証明するために電子透かし (ウォーターマーク (Watermark)) をコンテンツに挿入し、コンテンツを圧縮し、および暗号化し、コンテンツの取扱方針を生成し、署名データを付加してサービスプロバイダ3へ送信する。

サービスプロバイダ3は、専用のケーブルネットワーク、インターネット、ま

たは衛星通信などから構成されるネットワーク 4 を介して、コンテンツプロバイダ 2 から供給されたコンテンツに価格情報を追加し、署名データを付加して、ユーザホームネットワーク 5 に送信する。

ユーザホームネットワーク 5 は、サービスプロバイダ 3 から価格情報を付して送付されたコンテンツを入手し、コンテンツ利用権を購入し、購入処理を実行する。購入した利用権は、例えば再生利用権であったり、コピーする権利であったりする。そして、購入処理により生成された課金情報は、ユーザの保持する機器の、暗号処理部内の耐タンパメモリに保存され、ユーザホームネットワーク 5 が配送鍵  $K_d$  を電子配信サービスセンタ 1 から入手する際に、電子配信サービスセンタ 1 に送信される。

図 2 は、電子配信サービスセンタ 1 の機能の構成を示すブロック図である。サービスプロバイダ管理部 11 は、サービスプロバイダ 3 にサービスプロバイダ 3 の公開鍵証明書及び利益分配の情報を供給すると共に、必要に応じてコンテンツに付される情報（価格情報）を受信する。コンテンツプロバイダ管理部 12 は、コンテンツプロバイダ 2 に個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化した個別鍵  $K_i$  およびコンテンツプロバイダ 2 の公開鍵証明書を送信すると共に、利益分配の情報を供給し、必要に応じてコンテンツに付される情報（取扱方針）を受信する。著作権管理部 13 は、ユーザホームネットワーク 5 のコンテンツ利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers : 日本音楽著作権協会) に送信する。鍵サーバ 14 は、システム全てに使用する鍵の生成、保持、管理を行っており、例えば、コンテンツプロバイダ毎に異なる個別鍵  $K_i$  が生成されるとともに、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  も併せて生成され、これらはコンテンツプロバイダ管理部 12 を介してコンテンツプロバイダ 2 に供給され、さらに配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  も必要に応じて認証局 22 に供給され、配送鍵  $K_d$  はユーザ管理部 18 を介してユーザホームネットワーク 5 に供給される。ま

た、電子配信サービスセンタ 1 の公開鍵・秘密鍵、ユーザの保持する機器に固有の公開鍵・秘密鍵も全て生成、管理され、公開鍵は認証局 2 2 に送信され、公開鍵証明書作成に利用される。また、後述する暗号処理部 9 2 に固有の機器別 ID に応じた保存鍵  $K_{save}$  を生成、保持する場合もある。

電子配信サービスセンタ 1 からコンテンツプロバイダ 2 およびユーザホームネットワーク 5 を構成するホームサーバ 5 1（後述する）への、鍵の定期的な送信の例について、図 3 乃至図 6 を参照に説明する。図 3 は、コンテンツプロバイダ 2 がコンテンツの提供を開始し、ユーザホームネットワーク 5 を構成するホームサーバ 5 1 がコンテンツの利用を開始する、2000 年 1 月における、電子配信サービスセンタ 1 が有する配送鍵  $K_d$ 、個別鍵  $K_i$ 、コンテンツプロバイダ 2 が有する個別鍵  $K_i$ 、およびホームサーバ 5 1 が有する配送鍵  $K_d$  を示す図である。なお、以下省略するが、コンテンツプロバイダ 2 は、個別鍵  $K_i$  に対応する、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  も保持しているものとする。

図 3 の例において、配送鍵  $K_d$ 、個別鍵  $K_i$  は、暦の月の初日から月の末日まで、使用可能であり、例えば、所定のビット数の乱数である” a a a a a a a a a ” の値を有するバージョン 1 である配送鍵  $K_d$ 、” z z z z z z z z ” の値を有するバージョン 1 である個別鍵  $K_i$  は、2000 年 1 月 1 日から 2000 年 1 月 31 日まで使用可能（すなわち、2000 年 1 月 1 日から 2000 年 1 月 31 日の期間にサービスプロバイダ 3 がユーザホームネットワーク 5 に配布するコンテンツを暗号化するコンテンツ鍵  $K_c$  は、バージョン 1 である個別鍵  $K_i$  で暗号化され、バージョン 1 である個別鍵  $K_i$  は、バージョン 1 である配送鍵  $K_d$  で暗号化されている）であり、所定のビット数の乱数である” b b b b b b b b ” の値を有するバージョン 2 である配送鍵  $K_d$ 、” y y y y y y y y ” の値を有するバージョン 2 である個別鍵  $K_i$  は、2000 年 2 月 1 日から 2000 年 2 月 29 日まで使用可能（すなわち、その期間にサービスプロバイダ 3 がユーザホームネットワーク 5 に配布するコンテンツを暗号化するコンテンツ鍵  $K_c$  は、バージョン 2 である個別鍵  $K_i$  で暗号化され、バージョン 2 である個別鍵  $K_i$  は、バージ

ョン2である配送鍵 $K_d$ で暗号化されている)である。同様に、バージョン3である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年3月中に使用可能であり、バージョン4である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年4月中に使用可能であり、バージョン5である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年5月中に使用可能であり、バージョン6である配送鍵 $K_d$ 、個別鍵 $K_i$ は2000年6月中に使用可能である。

コンテンツプロバイダ2がコンテンツの提供を開始するのに先立ち、電子配信サービスセンタ1は、コンテンツプロバイダ2に、2000年1月から6月まで利用可能な、バージョン1乃至バージョン6の6つの個別鍵 $K_i$ と、それぞれを同一バージョンの配送鍵 $K_d$ で暗号化したものを送信し、コンテンツプロバイダ2は、6つの個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を受信し、記憶する。6月分の個別鍵 $K_i$ および配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を記憶するのは、コンテンツプロバイダ2は、コンテンツを提供する前のコンテンツおよびコンテンツ鍵 $K_c$ の暗号化などの準備に、所定の期間が必要だからである。

また、ホームサーバ51がコンテンツの利用を開始するのに先立ち、電子配信サービスセンタ1は、ホームサーバ51に2000年1月から2000年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送鍵 $K_d$ を送信し、ホームサーバ51は、3つの配送鍵 $K_d$ を受信し、記憶する。3月分の配送鍵 $K_d$ を記憶するのは、ホームサーバ51が、回線の混雑等を原因として、電子配信サービスセンタ1に接続できないなどのトラブルにより、コンテンツの購入が可能な契約期間にもかかわらずコンテンツが購入できない等の事態を避けるためであり、また、電子配信サービスセンタ1への接続の頻度を低くしたり、個々の機器の電子配信サービスセンタ1への同時アクセスを押さえ、電子配信サービスセンタ1の負荷を低減するためである。

2000年1月1日から2000年1月31日の期間には、バージョン1である配送鍵 $K_d$ および個別鍵 $K_i$ が、電子配信サービスセンタ1、コンテンツプロ

バイダ 2、ユーザホームネットワーク 5 を構成するホームサーバ 5 1 で利用される。

2000 年 2 月 1 における、電子配信サービスセンタ 1 の配送鍵  $K_d$  および個別鍵  $K_i$  のコンテンツプロバイダ 2、およびホームサーバ 5 1 への送信を図 4 で説明する。電子配信サービスセンタ 1 は、コンテンツプロバイダ 2 に、2000 年 2 月から 2000 年 7 月まで利用可能な、バージョン 2 乃至バージョン 7 の 6 つの個別鍵  $K_i$  と、それぞれを同一バージョンの配送鍵  $K_d$  で暗号化したものを送信し、コンテンツプロバイダ 2 は、6 つの個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を受信し、受信前に記憶していた個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  に上書きし、新たな個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を記憶する。電子配信サービスセンタ 1 は、ホームサーバ 5 1 に 2000 年 2 月から 2000 年 4 月まで、利用可能なバージョン 2 乃至バージョン 4 である 3 つの配送鍵  $K_d$  を送信し、ホームサーバ 5 1 は、3 つの配送鍵  $K_d$  を受信し、受信前に記憶していた配送鍵  $K_d$  に上書きし、新たな配送鍵  $K_d$  を記憶する。電子配信サービスセンタ 1 は、バージョン 1 ~ 7 である配送鍵  $K_d$  および個別鍵  $K_i$  をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵  $K_d$  を利用できるようにするためである。

2000 年 2 月 1 日から 2000 年 2 月 29 日の期間には、バージョン 2 である配送鍵  $K_d$  および個別鍵  $K_i$  が、電子配信サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するホームサーバ 5 1 で利用される。

2000 年 3 月 1 における、電子配信サービスセンタ 1 の配送鍵  $K_d$  および個別鍵  $K_i$  のコンテンツプロバイダ 2、およびホームサーバ 5 1 への送信を図 5 で説明する。電子配信サービスセンタ 1 は、コンテンツプロバイダ 2 に、2000 年 3 月から 2000 年 8 月まで利用可能な、バージョン 3 乃至バージョン 8 の 6 つの個別鍵  $K_i$  と、それぞれを同一バージョンの配送鍵  $K_d$  で暗号化したものを

送信し、コンテンツプロバイダ 2 は、6 つの個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を受信し、受信前に記憶していた個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  に上書きし、新たな個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を記憶する。電子配信サービスセンタ 1 は、ホームサーバ 51 に 2000 年 3 月から 2000 年 5 月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送鍵  $K_d$  を送信し、ホームサーバ 51 は、3 つの配送鍵  $K_d$  を受信し、受信前に記憶していた配送鍵  $K_d$  に上書きし、新たな配送鍵  $K_d$  を記憶する。電子配信サービスセンタ 1 は、バージョン 1 ~ 8 である配送鍵  $K_d$  および個別鍵  $K_i$  をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵  $K_d$  を利用できるようにするためである。

2000 年 3 月 1 日から 2000 年 3 月 31 日の期間には、バージョン 3 である配送鍵  $K_d$  および個別鍵  $K_i$  が、電子配信サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するホームサーバ 51 で利用される。

2000 年 4 月 1 における、電子配信サービスセンタ 1 の配送鍵  $K_d$  および個別鍵  $K_i$  のコンテンツプロバイダ 2、およびホームサーバ 51 への送信を図 6 で説明する。電子配信サービスセンタ 1 は、コンテンツプロバイダ 2 に、2000 年 4 月から 2000 年 9 月まで利用可能な、バージョン 4 乃至バージョン 9 の 6 つの個別鍵  $K_i$  と、それぞれを同一バージョンの配送鍵  $K_d$  で暗号化したものを送信し、コンテンツプロバイダ 2 は、6 つの個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を受信し、受信前に記憶していた個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  に上書きし、新たな個別鍵  $K_i$  および配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を記憶する。電子配信サービスセンタ 1 は、ホームサーバ 51 に 2000 年 4 月から 2000 年 6 月まで利用可能な、バージョン 4 乃至バージョン 6 である 3 つの配送鍵  $K_d$  を送信し、ホームサーバ 51 は、3 つの配送鍵  $K_d$  を受信し、受信前に記憶していた配送鍵  $K_d$  に上書きし、新たな配送鍵  $K_d$

を記憶する。電子配信サービスセンタ 1 は、バージョン 1 ～ 9 である配送鍵 K<sub>d</sub> および個別鍵 K<sub>i</sub> をそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送鍵 K<sub>d</sub> を利用できるようにするためである。

2000 年 4 月 1 日から 2000 年 4 月 30 日の期間には、バージョン 4 である配送鍵 K<sub>d</sub> および個別鍵 K<sub>i</sub> が、電子配信サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するホームサーバ 51 で利用される。

このように、あらかじめ先の月の配送鍵 K<sub>d</sub> および個別鍵 K<sub>i</sub> を配布しておくことで、仮にユーザが 1、2 ヶ月全くセンタにアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、センタにアクセスすることにより鍵を受信することができる。

電子配信サービスセンタ 1 の経歴データ管理部 15 (図 2) は、ユーザ管理部 18 が集めたコンテンツの利用の実績を示す情報である課金情報、必要に応じてそのコンテンツに対応する価格情報 (サービスプロバイダ 3 から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方)、および必要に応じてそのコンテンツに対応する取扱方針 (コンテンツプロバイダ 2 から送られてくるものと、ユーザが課金情報に付加して送ってくるものの、どちらか一方又は両方) を保持・管理し、サービスプロバイダ管理部 11 又はコンテンツプロバイダ管理部 12 等が課金情報や利用履歴等を利用する際にデータを出力する。なお、価格情報及び取扱方針は、課金情報に必要なデータが書き込まれている場合サービスプロバイダ 3 やコンテンツプロバイダ 2 から送られてこない場合がある。利益分配部 16 は、経歴データ管理部 15 から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、電子配信サービスセンタ 1、コンテンツプロバイダ 2、およびサービスプロバイダ 3 の利益を算出する。これらの情報は、出納部 20 へ供給され、出納部 20 を介して利益分配を行う場合もあるが、利益分配を行わず、これらの情報のみをサービスプロバイダ

管理部 1 1、コンテンツプロバイダ管理部 1 2、著作権管理部 1 3 に送信し、売上そのものはサービスプロバイダに入金させ、サービスプロバイダ 3 が各受益者に利益を分配する場合がある。相互認証部 1 7 は、コンテンツプロバイダ 2、サービスプロバイダ 3、およびユーザホームネットワーク 5 の所定の機器と後述する相互認証を実行する。

ユーザ管理部 1 8 は、ユーザ登録データベースを有し、ユーザホームネットワーク 5 の機器から登録の要求があったとき、ユーザ登録データベースを検索し、その記録内容に応じて、その機器を登録したり、または登録を拒否する等の登録情報を作成する。ユーザホームネットワーク 5 が電子配信サービスセンタ 1 と接続が可能な機能を有する複数の機器から構成されているとき、ユーザ管理部 1 8 は、登録情報に決済をする機器を規定し、決済 ID を登録し、更に、コンテンツの購入処理動作を規定したり、ユーザホームネットワークを構成する機器の範囲を規定したり、取引停止等の情報を規定し、ユーザホームネットワーク 5 の所定の機器（決済可能機器）に送信する。

図 7 に示すユーザ登録データベースの例は、ユーザホームネットワーク 5 内で構築されたネットワークグループ毎の登録状況を示したもので、各グループには、グループの ID を示すグループ ID、ホームネットワーク 5 を構成する機器に固有の ID、その ID に対応して（すなわち、その ID を有する機器毎に）、電子配信サービスセンタ 1 と接続が可能か否か、決済処理可能か否か、コンテンツの購入ができるか否か、決済処理を行うのはどの機器か、コンテンツの購入を依頼する機器はどれか、登録可能か否か、等の情報を記録する。

ユーザ登録データベースに記録されたグループ ID はユーザホームネットワーク毎に割り振られ、このグループ単位で決済、情報更新が行われる。従って、原則的にはグループ内の代表機器が電子配信サービスセンタ 1 と通信、決済処理、情報更新を一括して行い、グループ内の他の機器は電子配信サービスセンタ 1 とのやりとりを直接は行わない。ユーザ登録データベースに記録された ID は、機器毎に個別に割り振られた ID で、機器を識別するのに使用される。



ユーザ登録データベースに記録された電子配信サービスセンタ 1 と接続が可能か否かの情報は、その機器が、電子配信サービスセンタ 1 と物理的に接続が可能であるか否かを示し、接続できると記録された機器でも、決済処理可能であるとされた機器以外は、原則的に電子配信サービスセンタ 1 に接続されることがない（ただし、グループ内の代表機器が何らかの原因で決済処理動作しなくなった場合、代理で一時的に電子配信サービスセンタ 1 に接続されることはある）。また、接続ができないと記録された機器は、ユーザホームネットワーク 5 の決済処理可能な機器を介して、電子配信サービスセンタ 1 に、課金情報等を出力する。

ユーザ登録データベースに記録された決済処理が可能か否かの情報は、その機器が、決済可能か否かを示す。ユーザホームネットワーク 5 が、コンテンツの利用権の購入などが可能な複数の機器で構成されているとき、その中の決済処理が可能である 1 台の機器は、電子配信サービスセンタ 1 に、ユーザホームネットワーク 5 の電子配信サービスセンタ 1 に登録されている全ての機器の、課金情報、必要に応じて価格情報、および取扱方針を送信し、決済処理の完了に応じて電子配信サービスセンタ 1 から配送鍵  $K_d$ 、登録情報を受信する。こうすることで、機器毎に処理を行うのに比べ、電子配信サービスセンタ 1 の処理が軽減される。

ユーザ登録データベースに記録された購入処理が可能か否かの情報は、その機器が、コンテンツの利用権の購入ができるか否かを表す。購入不可の機器においては、他の購入可の機器から利用権の代理購入（別の機器で権利を購入し、その権利を全て譲り受けるものを言う。供給側には全く権利は残らない）、再配布（既に購入したコンテンツの利用権を、同一利用権内容または異なる利用権内容でもう一度購入し、別機器に供給する方式を言う。このとき、供給側には全く権利は残らない。再配布は、割引を行うことを主たる目的とする。割引の特典を受けられるのは、同一決済 ID を使用しているグループであることが条件である。なぜなら、同一決済 ID に属するグループ内の処理においては、電子配信サービスセンタ 1 の処理負担が軽減され、従って、その代償として割引が受けられるからである）または管理移動（コンテンツ再生権、特に無期限再生権の移動ができる

が、再生権送信器においては再生権受信器がどの機器であるか管理され、再生権の返還がない場合、再度管理移動ができず、再生権受信器においては、再生権送信器がどの機器であるかが管理され、再度管理移動が全くできず、唯一、再生権を与えてくれた再生権送信器に再生権を返還することのみできる）を行ってもらってコンテンツ利用権を取得する。

ここで、コンテンツの利用方法／利用権及び購入方法について簡単に説明する。コンテンツの利用方法としては、コンテンツの利用権を自己で管理保持しているものが利用する場合と、他機器の保持する利用権を行使して自己の機器において利用する、2つのものがある。コンテンツの利用権としては、無制限再生権（コンテンツの再生期間及び回数に制限がないもの、なお、音楽コンテンツの場合は再生であるが、ゲームプログラム等では実行になる）、時間制限付き再生権（コンテンツの再生できる期間が限られているもの）、回数制限付き再生権（コンテンツの再生できる回数が限られているもの）、無制限複製権（コンテンツの複製期間及び回数に制限がないもの）、回数制限付き複製権（コンテンツの複製に回数制限があるもの）（複製権には、コピー管理情報なし複製権、コピー管理情報付き複製権（SCMS）等、その他専用メディア向け複製権等がある）（また時間制限付き複製権もある場合がある）、管理移動権がある。そして、利用権の購入方法としては、これらの利用権を直接購入する通常の購入に加え、既に購入した利用権の内容を別の内容に変更する利用権内容変更、他の機器で既に購入した権利に基づき利用権を別途購入する再配布、他の機器で利用権の購入を代理で行ってもらう代理購入、複数のコンテンツ利用権を一括して購入管理するアルバム購入等がある。

ユーザ登録データベースに記録された代理決済者に記された情報は、コンテンツの利用権を購入した際に生成した課金情報を、代理で電子配信サービスセンタ1に送信してもらう機器のIDを示す。

ユーザ登録データベースに記録された代理購入者に記された情報は、コンテンツの利用権の購入ができない機器に対し、代理で利用権の購入を行ってくれる機

器のIDを示す。ただし、購入処理可能なグループ内機器全てが代理購入者ということにしていた場合には、特に記録しておく必要はない。

ユーザ登録データベースに記録された登録が可能か否かの情報は、決済機関（例えば、銀行）、またはクレジットカード会社などから供給される料金の未払い、不正処理等の情報を基に、更新される。登録が不可と記録されたIDを有する機器の登録の要求に対して、ユーザ管理部18は、その登録を拒否し、登録を拒否された機器は、以降、このシステムのコンテンツの購入ができただけでなく、ユーザホームネットワーク5内の他機器とのデータ送受信もできなくなる。また場合によっては購入済のコンテンツの利用も制限される場合がある（ただし、電子配信サービスセンタ1等に機器を持ち込み、検査等を済ませた後再登録されることはある）。また、「登録可」、「登録不可」だけでなく、「決済未処理」、「一時停止」等の状態もあり得る。

また、ユーザ管理部18は、ユーザホームネットワーク5の機器から課金情報、登録情報、必要に応じて価格情報や取扱方針が供給され、課金情報、価格情報、および取扱方針を経歴データ管理部15に出力し、ユーザホームネットワーク5の機器に、配送鍵K<sub>j</sub>、登録情報を供給する。供給されるタイミングについては後述する。

ここで、図8を用いて登録情報を説明する。図8の登録情報はユーザ登録データベースの情報に加え、決済IDおよび署名が付加されており、同一決済グループの情報のみが含まれている。決済IDとは、決済を行う際に課金請求部19および出納部20が使用するユーザの、ユーザ情報データベース（例えば銀行口座番号やクレジットカード番号）内のIDを示している。署名の生成については、後述する。

再び図2にもどり、課金請求部19は、経歴データ管理部15から供給された、課金情報、必要に応じて価格情報、および取扱方針に基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。また、必要に応じてユーザ管理部18を介してユーザに決済情報を提供する。出納部20は、ユーザ、コンテン

ツプロバイダ 2、およびサービスプロバイダ 3 への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決済処理を実行する。なお、出納部 20 は、サービスプロバイダ 3 へ売上のすべてを送金させ、利益分配部 16 を介して送信された分配金情報をもとに、サービスプロバイダ 3 が利益分配をする場合がある。監査部 21 は、ユーザホームネットワーク 5 の機器から供給された課金情報、価格情報、および取扱方針を、コンテンツプロバイダ 2 から供給された取扱方針と、サービスプロバイダ 3 から供給された価格情報とからその正当性を監査する。

また、監査部 21 の処理としては、ユーザホームネットワーク 5 から入金された金額と、利益分配した合計金額又はサービスプロバイダ 3 へ送った金額との整合性を監査する処理や、ユーザホームネットワーク 5 の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダ ID、サービスプロバイダ ID や考えられない取り分、価格等が含まれているか否かを監査する処理がある。

認証局 22 は、鍵サーバ 14 から供給された公開鍵の証明書を生成し、コンテンツプロバイダ 2、サービスプロバイダ 3 へ供給し、ユーザ機器製造時にホームサーバ 51 の大容量記憶部 68（後述する）や、据置機器 52 の小容量記憶部 75（後述する）に保存される公開鍵証明書も生成する。コンテンツプロバイダ 2 がコンテンツのオーサリングを行わない場合、これを代替える方法として、コンテンツを保持するコンテンツサーバ 23、コンテンツオーサリング 24 がある。

図 9 は、コンテンツプロバイダ 2 の機能の構成を示すブロック図である。コンテンツサーバ 31 は、ユーザに供給するコンテンツを記憶し、電子透かし（ウォーターマーク）付加部 32 に供給する。電子透かし付加部 32 は、コンテンツサーバ 31 から供給されたコンテンツに自分の所有物であることを示すコンテンツプロバイダ ID を電子透かしの形で挿入し、圧縮部 33 に供給する。圧縮部 33 は、電子透かし付加部 32 から供給されたコンテンツを、ATRAC（

Adaptive Transform Acoustic Coding) (商標) 等の方式で圧縮し、コンテンツ暗号部 34 に供給する。因に、圧縮方式としては ATRAC に代えて MP3 や AAC 等の方式を用いることができる。コンテンツ暗号部 34 は、圧縮部 33 で圧縮されたコンテンツを、コンテンツ鍵生成部 35 から供給された鍵 (以下、この鍵をコンテンツ鍵  $K_c$  と称する) を用いて、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果を署名生成部 38 に出力する。

コンテンツ鍵生成部 35 は、コンテンツ鍵  $K_c$  となる所定のビット数の乱数を生成し、この中で弱鍵 (例えば、 $K_c = 1E1E1E1E0E0E0E0E$  や  $1EE01EE00EF00EF0$  など) と呼ばれる暗号化に不適なビット列を除いたものをコンテンツ暗号部 34、コンテンツ鍵暗号部 36 に供給する。そのような不適なビット列がない暗号アルゴリズムを使用するときは、不適なビット列を除く処理は不要である。コンテンツ鍵暗号部 36 は、コンテンツ鍵  $K_c$  を電子配信サービスセンタ 1 から供給された個別鍵  $K_i$  を使用して、DES などの共通鍵暗号方式で暗号化し、その結果を署名生成部 38 に出力する。因に、暗号化方式としては、DES に限らず、例えば RSA (Rivest, Shamir, Adleman) 等の公開鍵暗号方式を用いるようにしても良い。

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分 (データ攪拌部) と、データ攪拌部で使用する鍵 (拡大鍵) を共通鍵から生成する部分 (鍵処理部) からなる。DES の全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文 64 ビットは、上位 32 ビットの  $H0$ 、および下位 32 ビットの  $L0$  に分割される。鍵処理部から供給された 48 ビットの拡大鍵  $K1$ 、および下位 32 ビットの  $L0$  を入力として、下位 32 ビットの  $L0$  を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成される。次

に、上位32ビットのH0と、F関数の出力が排他的論理和され、その結果はL1とされる。L0は、H1とされる。

上位32ビットのH0および下位32ビットのL0を基に、以上の処理を16回繰り返す、得られた上位32ビットのH16および下位32ビットのL16が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることによって実現される。

なお、本実施の形態では共通鍵暗号としてDESを示したが、NTT（商標）が提案するFEAL（Fast Encryption Algorithm）、IDEA（International Data Encryption Algorithm）、E2や、米国次期暗号標準であるAES（Advanced Encryption Standard）など、いずれでもよい。

取扱方針生成部37は、コンテンツの取扱方針を生成し、暗号化されるコンテンツに対応して、取扱方針を署名生成部38に出力する。なお、取扱方針生成部37は、生成した取扱方針を図示せぬ通信手段を介して電子配信サービスセンタ1に供給する場合があります、そのデータは保持・管理されている。署名生成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{co}$ 、暗号化された個別鍵 $K_i$ 、取扱方針に電子署名を付加し、コンテンツプロバイダ2の証明書 $C_c p$ と共にサービスプロバイダ3に送信する（以降、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{co}$ 、暗号化された個別鍵 $K_i$ 、取扱方針のそれぞれにコンテンツプロバイダ3の秘密鍵を使用して電子署名を付加したものを、コンテンツプロバイダセキュアコンテナと称する）。なお、個々のデータに署名を別々に付加するのではなく、データ全体に対して1つの署名を付けるようにしてもよい。

相互認証部39は、電子配信サービスセンタ1と相互認証し、また、必要に応じてサービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証する。メモリ40Aは、コンテンツ

ロバイダ2が秘密裏に保持しなくてはならない個別鍵 $K_i$ を保持するため、第3者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ40Bは、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、コンテンツプロバイダ2の公開鍵証明書が保存されるだけであるため、通常の記憶装置等何でもよい（公開情報であるため、秘密にする必要がない）。なお、メモリ40A、40Bを一つにしてもかまわない。

署名は、データまたは後述する証明書に付け、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵を使用して作成される。

ハッシュ関数および署名について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD (Message Digest) 4、MD5、SHA (Secure Hash Algorithm) -1などが用いられる。

データと署名を送信する送信装置（コンテンツプロバイダ2）の署名生成部38は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を生成する。この処理を、図10を用いて説明する（EC-DSA (Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3）。ステップS1で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、 $K_s$ を秘密鍵（ $0 < K_s < r$ ）とする。ステップS2で乱数uを $0 < u < r$ になるように乱数発生ユニットで生成する。ステッ

プ S 3 でベースポイントを  $u$  倍した座標を計算する。なお、楕円曲線上の加算、2 倍算は次のように定義されている。

$P = (X_0, Y_0)$ 、 $Q = (X_1, Y_1)$ 、 $R = (X_2, Y_2) = P + Q$  とし、 $P \neq Q$  の時、

$$X_2 = \lambda^2 - X_0 - X_1$$

$$Y_2 = \lambda (X_0 - X_2) - Y_0$$

$$\lambda = (Y_1 - Y_0) / (X_1 - X_0)$$

$P = Q$  の時、

$$X_2 = \lambda^2 - 2 X_0$$

$$Y_2 = \lambda (X_0 - X_2) - Y_0$$

$$\lambda = (3 X_0^2 + a) / 2 Y_0$$

となり、これらを用いて点  $G$  の  $u$  倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。 $G$ 、 $2G$ 、 $4G \cdots$  を計算し、 $u$  を 2 進数展開して 1 が立っているところに対応する  $(2^i) \times G$  を加算する（ $i$  は  $u$  の L S B から数えた時のビット位置））。ステップ S 4 で  $c = X_v \bmod r$  を計算し、ステップ S 5 でこの値が 0 になるかどうか判定し、0 でなければステップ S 6 へと進み、メッセージ  $M$  のハッシュ値を計算し、 $f = \text{SHA-1}(M)$  とする。次に、ステップ S 7 において、 $d = [(f + c K_s) / u] \bmod r$  を計算し、ステップ S 8 で  $d$  が 0 であるかどうか判定する。 $d$  が 0 出なければ、 $c$  および  $d$  を署名データとする。仮に、 $r$  を 160 ビット長の長さであると仮定すると、署名データは 320 ビット長となる。

ステップ S 5 において、 $c$  が 0 であった場合、ステップ S 2 に戻って新たな乱数を生成し直す。同様に、ステップ S 8 で  $d$  が 0 であった場合も、ステップ S 2 に戻って乱数を生成し直す。

署名とデータを受信した受信装置（ユーザホームネットワーク 5）は、例えば、公開鍵暗号方式である楕円曲線暗号を用いて署名を検証する。この処理を、図 11 を用いて説明する。（受信装置は）ステップ S 10 で、 $M$  をメッセージ、 $p$



を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $G$ および $K_s G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS11で署名データ $c$ および $d$ が $0 < c, d < r$ を満たすか検査する。これを満たしていた場合、ステップS12で、メッセージ $M$ のハッシュ値を計算し、 $f = \text{SHA-1}(M)$ とする。次に、ステップS13で $h = 1/d \bmod r$ を計算し、ステップS14で $h_1 = fh$ 、 $h_2 = ch \bmod r$ を計算する。ステップS15において、既に計算した $h_1$ および $h_2$ を用い、 $P = (X_p, Y_p) = h_1 G + h_2 K_s G$ を計算する。署名検証者は、公開鍵 $G$ および $K_s G$ を知っているので、ステップS3と同様にこの計算ができる。そして、ステップS16で $P$ が無限遠点かどうか判定し、無限遠点でなければステップS17に進む（実際には、無限遠点の判定はステップS15ですべてしてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、前述の $\lambda$ が計算できず、 $R$ が無限遠点であることが判明している。ステップS17で $X_p \bmod r$ を計算し、署名データ $c$ と比較する。この値が一致していた場合、ステップS18に進み、署名が正しいと判定する。

署名が正しいと判定された場合、受信データは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータであることがわかる。

ステップS11において、署名データ $c$ および $d$ が $0 < c, d < r$ を満たさなかった場合、ステップS19に進む。また、ステップS16において、 $P$ が無限遠点であった場合もステップS19に進む。さらにまた、ステップS17において、 $X_p \bmod r$ の値が、署名データ $c$ と一致していなかった場合にもステップS19に進む。ステップS19において、署名が正しくないと判定する。

署名が正しくないと判定された場合、受信データは改竄されているか、公開鍵に対応した秘密鍵を保持する送信装置から送信されたデータではないことがわかる。

なお、本実施の形態では、ハッシュ関数としてSHA-1を使用した。MD4、MD5などいずれの関数を使用してもよい。また、署名の生成および検証は

R S A暗号を用いて行ってもよい (A N S I X 9 . 3 1 - 1)。

次に公開鍵暗号方式の暗号化・復号化について説明する。暗号化および復号化で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対して、公開鍵暗号方式は、暗号化に使用する鍵と復号化に使用する鍵が異なる。公開鍵暗号方式を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開してもよい鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号方式の中で代表的な楕円曲線暗号化方法を説明する。図12において、ステップS20で、 $M_x$ 、 $M_y$ をメッセージ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $G$ および $K_s$ 、 $G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS21で乱数 $u$ を $0 < u < r$ になるように生成する。ステップS22で公開鍵 $K_s$ 、 $G$ を $u$ 倍した座標 $V$ を計算する。なお、楕円曲線上のスカラー倍は署名生成のところで説明した方法と同一のため、ここでは説明を省略する。ステップS23で、 $V$ の $X$ 座標を $M_x$ 倍して $p$ で剰余を求め $X_0$ とする。ステップS24で $V$ の $Y$ 座標を $M_y$ 倍して $p$ で剰余を求め $Y_0$ とする。なお、メッセージの長さが $p$ のビット数より少ない場合、 $M_y$ は乱数を使い、復号部では $M_y$ を破棄するようにする。ステップS25において、 $uG$ を計算し、ステップS26で暗号文 $uG$ 、( $X_0$ 、 $Y_0$ )を得る。

ここで公開鍵暗号方式の復号化について、図13を用いて説明する。ステップS30において、 $uG$ 、( $X_0$ 、 $Y_0$ )を暗号文データ、 $p$ を標数、 $a$ 、 $b$ を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 $G$ を楕円曲線上のベースポイント、 $r$ を $G$ の位数、 $K_s$ を秘密鍵（ $0 < K_s < r$ ）とする。ステップS31において、暗号データ $uG$ を秘密鍵 $K_s$ 倍する。ステップS32では、暗号データの内、( $X_0$ 、 $Y_0$ )の $X$ 座標を取り出し、 $X_1 = X_0 / X_v \mod p$ を計算する。ステップS33においては、 $Y_1 = Y_0 / Y_v \mod p$ を計算する。そして、ステップS34で $X_1$ を $M_x$ とし、 $Y_1$ を $M_y$ としてメッセージを取り出す。この時、 $M_y$ をメッセージにしていなかった場合、 $Y_1$ は破棄する。

このように公開鍵暗号方式では、秘密鍵を $K_s$ 、公開鍵を $G$ 、 $K_s$ 、 $G$ とすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

また、公開鍵暗号方式の他の例としてはRSA暗号（R i v e s t、S h a m i r、A d l e m a n）が知られている。

図14は、サービスプロバイダ3の機能の構成を示すブロック図である。コンテンツサーバ41は、コンテンツプロバイダ2から供給された、コンテンツプロバイダ2の公開鍵証明書および暗号化されているコンテンツを記憶している。コンテンツプロバイダ2の公開鍵証明書は、証明書検査部42で、証明書内の署名が認証局22の公開鍵で検証され、検証に成功した場合、コンテンツプロバイダ2の公開鍵を署名検証部43に供給する。署名検証部43においては、コンテンツサーバ41に記憶されている取扱方針に対するコンテンツプロバイダ2の署名を、先ほど検証したコンテンツプロバイダ2の公開鍵を用いて検証し、検証に成功した場合、取扱方針を値付け部44に供給する。値付け部44においては、取扱方針から価格情報を作成し、署名生成部45に供給する。署名生成部45においては、図示せぬ耐タンパメモリ（コンテンツプロバイダ2内の40Aと同様）に保持されたサービスプロバイダ3の秘密鍵を用い、価格情報に対する署名を生成する（以降、コンテンツプロバイダセキュアコンテナおよび価格情報にサービスプロバイダ3の秘密鍵を用いて電子署名を付加したものを、サービスプロバイダセキュアコンテナと称する）。なお、価格情報に署名を付加するのではなく、コンテンツプロバイダセキュアコンテナと価格情報全体に対して1つの署名を生成するようにしてもよい。そして、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書を、ネットワーク4（図1）を介してユーザホームネットワーク5へ供給する。相互認証部46は、電子配信サービスセンタ1と相互認証し、また、必要に応じてコンテンツプロバイダ、およびインターネット、ケーブル通信等を介し、可能であればユーザホームネットワーク5と相互認証する。

図15は、ユーザホームネットワーク5の構成を示すブロック図である。ホームサーバ51は、ネットワーク4を介して、サービスプロバイダ3からコンテンツを含んだセキュアコンテナを受信し、コンテンツの利用権を購入し、その権利を行使してコンテンツの復号、伸張、再生、複製を行う。

通信部61は、ネットワーク4を介してサービスプロバイダ3、または電子配信サービスセンタ1と通信し、所定の情報を受信し、または送信する。上位コントローラ62は、入力手段63からの信号を受信し、所定のメッセージ等を表示手段64に表示し、暗号処理部65を利用してコンテンツの利用権購入処理等を行い、伸張部66に大容量記憶部68から読み出した暗号化されたコンテンツを供給し、大容量記憶部68に暗号化されたコンテンツ等を記憶する。入力手段63は、リモートコントローラからの信号や入力ボタンからの入力データを上位コントローラ62に送信する。表示手段64は、液晶表示器のような表示デバイスで構成され、ユーザに指示を出したり、情報を表示したりする。入力手段63および表示手段64は、必要に応じてタッチパネル式液晶表示器などになり、一つにまとめられる場合がある。暗号処理部65は、サービスプロバイダ3、または電子配信サービスセンタ1若しくはその他の機器の暗号処理部と相互認証し、コンテンツ利用権を購入すると共に、所定のデータの暗号化／復号化を行い、コンテンツ鍵 $K_{co}$ および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵 $K_d$ 、課金情報等を記憶する。伸張部66は、暗号処理部65と相互認証してコンテンツ鍵 $K_{co}$ を受信し、このコンテンツ鍵 $K_{co}$ を用いて上位コントローラ62から供給された暗号化されたコンテンツを復号化し、ATRAC等の所定の方式で伸張し、さらに所定の電子透かしをコンテンツに挿入する。外部メモリ67は、フラッシュメモリ等の不揮発メモリやバックアップ電源付き揮発性メモリで構成され、保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ および使用許諾条件情報を保存する。大容量記憶部68はHDDや光ディスク等の記憶デバイスで、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナ（暗号化されたコンテンツ、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 、

配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、取扱方針、価格情報及びそれらの署名)、公開鍵証明書、登録情報等が保存されている。

電子配信サービスセンタ 1 と相互認証し、コンテンツ利用権を購入すると共に課金情報を生成し、所定のデータの復号化/暗号化を行い、コンテンツ鍵 $K_c$ および使用許諾条件情報を保持する外部メモリを管理し、さらに配送鍵 $K_d$ 、課金情報等を記憶する暗号処理部 6 5 は、制御部 9 1、記憶モジュール 9 2、登録情報検査モジュール 9 3、購入処理モジュール 9 4、相互認証モジュール 9 5、暗号/復号化モジュール 9 6、および外部メモリ制御部 9 7 から構成される。この暗号処理部 6 5 は、シングルチップの暗号処理専用 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性(耐タンパ性)を有する。

制御部 9 1 は、上位コントローラ 6 2 からのコマンドに応じて各モジュールを制御すると共に、各モジュールからの結果を上位コントローラ 6 2 に返送する。記憶モジュール 9 2 は、購入処理モジュール 9 4 から供給された課金情報、および配送鍵 $K_d$ 等のデータを記憶し、他の機能ブロックが所定の処理を実行するとき、配送鍵 $K_d$ 等のデータを供給する。登録情報検査モジュール 9 3 は、上位コントローラ 6 2 から供給された登録情報を検査し、ユーザホームネットワーク 5 内の他の機器と相互認証するか否か、課金情報の授受をすべきか否か、コンテンツの再配布等をすべきか否かの判断を行う。購入処理モジュール 9 4 は、サービスプロバイダ 3 から受信したセキュアコンテナに含まれる取扱方針および価格情報(並びに、場合によっては、既に保持している使用許諾条件情報)から、新たに使用許諾条件情報を生成して外部メモリ制御部 9 7 又は制御部 9 1 に出力し、課金情報を生成して記憶モジュール 9 2 に出力する。相互認証モジュール 9 5 は、電子配信サービスセンタ 1、ホームネットワーク 5 内の他の機器の暗号処理部および伸張部 6 6 との相互認証を実行し、必要に応じて、一時鍵 $K_{temp}$ (セッション鍵)を生成し、暗号/復号化モジュール 9 6 に供給する。

復号／暗号化モジュール 96 は、復号化ユニット 111、暗号化ユニット 112、乱数発生ユニット 113、署名生成ユニット 114、および署名検証ユニット 115 から構成される。復号化ユニット 111 は、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  を復号化したり、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  を復号化したり、一時鍵  $K_{temp}$  で暗号化された各種データを復号化したりする。暗号化ユニット 112 は、復号化されたコンテンツ鍵  $K_c$  を、記憶モジュール 92 に保持されている保存鍵  $K_{save}$  で暗号化し、制御部 91 を介して外部メモリ制御部 97 に出力したり、一時鍵  $K_{temp}$  で各種データを暗号化したりする。乱数発生ユニット 113 は、所定の桁数の乱数を発生し、相互認証モジュール 95 や署名生成ユニット 114 に供給する。署名生成ユニット 114 は、制御部 91 から供給されたメッセージのハッシュ値を計算し、乱数発生ユニット 113 から供給された乱数を用いて署名データを生成して制御部 91 に出力する。署名検証ユニット 115 は、制御部から供給されたメッセージおよび署名データから署名が正しいかどうか判定し、その結果を制御部 91 に出力する。なお、署名の生成／検証方法については図 10、図 11 について上述した場合と同様である。

外部メモリ制御部 97 は、外部メモリ 67 を制御してデータの読み書きを行い、外部メモリ内のデータが改竄されていないかどうかデータ検証を行う。図 16 は、外部メモリ制御部 97 の動作を説明するブロック図である。図 16 において、記憶モジュール 92 には、N 個の改竄防止用ハッシュ値 (Integrity Check Value) が保存されている。外部メモリ 67 は、N ブロックのデータ領域に分割されており、それぞれのデータ領域には M 組のコンテンツ鍵  $K_c$  および使用許諾条件情報が書き込めるようになっている。また、外部メモリ 67 には、自由に使用できるその他の領域も用意されている。改竄防止用ハッシュ値 ICV は、それに対応する外部メモリ 67 内の全データに対するハッシュ値になっている。外部メモリの読み出し手順および書き込み手順については、フローチャートを用いて後述する。

コンテンツを復号化し、伸張し、所定の電子透かしを付加する伸張部 66 (図

15) は、相互認証モジュール101、鍵復号モジュール102、復号モジュール103、伸張モジュール104、電子透かし付加モジュール105、および記憶モジュール106から構成される。相互認証モジュール101は、暗号処理部65と相互認証し、一時鍵 $K_{temp}$ を鍵復号モジュール102に出力する。鍵復号モジュール102は、外部メモリ67から読み出され一時鍵 $K_{temp}$ で暗号化されているコンテンツ鍵 $K_{co}$ を一時鍵 $K_{temp}$ で復号化し、復号モジュール103に出力する。復号モジュール103は、大容量記憶部68に記録されたコンテンツをコンテンツ鍵 $K_{co}$ で復号化し、伸張モジュール104に出力する。伸張モジュール104は、復号化されたコンテンツを、更にATRAC等の方式で伸張し、電子透かし付加モジュール105に出力する。電子透かし付加モジュール105は、購入処理を行った暗号処理部の個別IDを電子透かし技術を用いてコンテンツに挿入し、他の機器や図示せぬスピーカに出力し、音楽を再生する。

記憶モジュール106には、暗号処理部65との相互認証に必要な鍵データが保存されている。なお、伸張部66は、耐タンパ性を備えていることが望ましい。

外部メモリ67は、購入処理モジュール94で権利購入した際に生成した使用許諾条件情報や保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ を記憶している。大容量記憶部68は、サービスプロバイダ3から供給されたセキュアコンテナや公開鍵証明書、登録情報等を記録する。

装着された光ディスク、半導体メモリ等の記録メディア80にサービスプロバイダ3から供給されたコンテンツを記録し、再生する据置機器52は、通信部71、上位コントローラ72、暗号処理部73、伸張部74、小容量記憶部75、記録再生部76、入力手段77、表示手段78、外部メモリ79、および記録メディア80から構成される。通信部71は通信部61と同じ機能を有し、その説明は省略する。上位コントローラ72は上位コントローラ62と同じ機能を有し、その説明は省略する。暗号処理部73は暗号処理部65と同じ機能を有し、その説明は省略する。伸張部74は伸張部66と同じ機能を有し、その説明は省略する。

する。小容量記憶部 75 は大容量記憶部 68 と同じ機能を有しているものの、コンテンツそのものは保存されず、公開鍵証明書や登録情報等が記憶されるだけである。記録再生部 76 は、光ディスク、半導体メモリ等の記録メディア 80 が装着され、その記録メディア 80 にコンテンツを記録し、読み出したコンテンツを伸張部に出力する。入力手段 77 は入力手段 63 と同じ機能を有し、その説明は省略する。表示手段 78 は表示手段 64 と同じ機能を有し、その説明は省略する。外部メモリ 79 は外部メモリ 67 と同じ機能を有し、その説明は省略する。記録メディア 80 は、例えば MD (Mini Disk : 商標) や、電子配信専用記憶メディア (半導体メモリを用いた Memory Stick : 商標) であつたりする。

ユーザが携帯し、音楽を再生して楽しむための機器である携帯機器 53 は、通信部 81、上位コントローラ 82、暗号処理部 83、伸張部 84、および外部メモリ 85 から構成される。通信部 81 は通信部 61 と同じ機能を有し、その説明は省略する。上位コントローラ 82 は上位コントローラ 62 と同じ機能を有し、その説明は省略する。暗号処理部 83 は暗号処理部 65 と同じ機能を有し、その説明は省略する。伸張部 84 は伸張部 66 と同じ機能を有し、その説明は省略する。外部メモリ 85 は外部メモリ 67 と同じ機能を有し、その説明は省略する。ただし、これらのメモリは半導体メモリだけとは限らず、HDD、書き換え可能な光ディスク等いずれでもよい。

図 17 は、電子配信専用の記録メディアの構成図を示したものである。電子配信されたコンテンツを保存する記録メディア 120 は、通信部 121、暗号処理部 122、および外部メモリ 123 から構成される。通信部 121 は、据置機器 52 (図 15) の記録再生部 76 とデータの送受信を行う。据置機器 52 と相互認証し、コンテンツ利用権を譲り受け、所定のデータの復号化/暗号化を行い、コンテンツ鍵  $K_{co}$  および使用許諾条件情報等を保持する外部メモリを管理し、さらに保存鍵  $K_{save}$  等を記憶する暗号処理部 122 は、その構成は暗号処理部 65 と同じ機能を有し、その説明は省略する。外部メモリ 123 は、保存鍵  $K_{save}$  で



暗号化されたコンテンツ鍵 $K_{co}$ 、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、コンテンツの使用条件を定めた使用許諾条件情報、必要に応じて取扱方針、および価格情報を記憶している。

電子配信専用記録メディア120は、据置機器52の時に説明した記録メディアとは使い方が異なっている。通常の記録メディア80は、ホームサーバ51の大容量記憶部68の代用品であるのに対し、電子配信専用メディア120は、伸張部を持たない携帯機器に異ならない。従って、コンテンツの再生を行う際には、伸張部74をもつ据置機器52のような機器が必要であるが、コンテンツを譲り受けたり、コンテンツを管理したりする機能に関してはホームサーバ51や携帯機器53と同様な処理ができる。これらの違いにより、通常の記録メディア80に記録されたコンテンツは、記録した機器以外では再生することができないものの、電子配信専用記録メディア120に記録されたコンテンツは、記録した機器以外の機器でも再生できるようになる。すなわち、通常の記録メディア80には、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツがあるだけなので、コンテンツ鍵 $K_{co}$ を持つ（記録した）機器以外では再生ができない。一方、電子配信専用記録メディア120においては、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツだけでなく、コンテンツ鍵 $K_{co}$ も、電子配信専用記録メディア120個有の保存鍵 $K_{save}$ で暗号化されて保持されているため、他の機器で再生することが可能になる。

つまり暗号処理部122の相互認証モジュール128と据置機器52の暗号処理部73の図示せぬ相互認証モジュール間で相互認証を行った後、専用記録メディア固有の保存鍵 $K_{save3}$ でコンテンツ鍵 $K_{co}$ を復号化し、共有した一時鍵 $K_{temp}$ でコンテンツ鍵 $K_{co}$ を暗号化し、暗号処理部73へ送信して再生する。

図18は、各機器内のデータ記憶状況を示すブロック図である。ホームサーバ51において、暗号処理部65内の記憶モジュール92には、機器を特定するための個別ID（暗号処理部を特定するものと同一）、課金処理する際に使用する決済用ID（必要に応じて個別IDで代替えできるし、登録情報にあるので不要

の場合もある)、機器毎に異なる秘密鍵、保存鍵 $K_{save}$ 、電子配信サービスセンタ 1 と相互認証する際に使用する電子配信サービスセンタ 1 の公開鍵 (電子配信サービスセンタ 1 の公開鍵証明書があれば不要)、公開鍵証明書を検証するための認証局 2 2 の公開鍵、伸張部 6 6 と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。これに対し、電子配信サービスセンタ 1 から定期的に配布される配送鍵 $K_d$ 、購入処理の際に書き込まれる課金情報、外部メモリ 6 7 内に保持するコンテンツ鍵 $K_{co}$ および使用許諾条件情報の改竄チェック用のハッシュ値は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶モジュール 9 2 に記憶されている。伸張部 6 6 内の記憶モジュール 1 0 6 には、伸張部を特定するための個別 ID、暗号処理部 6 5 と相互認証する際に使用する共通鍵が、機器製造時に予め記憶される。なお、暗号処理部 6 5 と伸張部 6 6 を 1 対 1 に対応させるため、それぞれの記憶モジュールに互いの ID を持たせておいても良い (相互認証が共通鍵で行われているため、結果的には対応した暗号処理部、伸張部でしかやりとりができない。但し処理としては公開鍵暗号方式の相互認証であっても良い。このとき保存されている鍵は共通鍵ではなく、伸張部 6 6 固有の秘密鍵になる)。

外部メモリ 6 7 には、コンテンツの復号を行う際に使用する保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、そのコンテンツ鍵 $K_{co}$ を利用する際の条件を示す使用許諾条件情報が記憶されている。また、大容量記憶部 6 8 には、記憶モジュール 9 2 内にある機器個別の秘密鍵に対応する公開鍵の証明書 (機器の公開鍵証明書)、登録情報、コンテンツプロバイダセキュアコンテナ (コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツおよびその署名、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ およびその署名、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ およびその署名、取扱方針およびその署名)、サービスプロバイダセキュアコンテナ (価格情報およびその署名)、コンテンツプロバイダ 2 の公開鍵証明書、サービスプロバイダ 3 の公開鍵証明書が記憶されている。

携帯機器 5 3 には、ホームサーバ 5 1 が保持する暗号処理部 6 5 と同一の暗号

処理部 8 3、外部メモリ 6 7 と同一の外部メモリ 8 5 が備えられている（内部データが同一のものは省略されている。例えば、伸張部）。しかし、その内部に保持されるデータは、図に示すように若干異なっている。暗号処理部 8 3 内の記憶モジュールの保持するデータは、機器を特定するための個別 ID、機器毎に異なる秘密鍵、保存鍵  $K_{save}$ 、電子配信サービスセンタ 1 と相互認証する際に使用する、電子配信サービスセンタ 1 の公開鍵（ただし、ホームサーバ 5 1 に電子配信サービスセンタ 1 との手続きを全て代行してもらう場合は必要ない）、公開鍵証明書を検証するための認証局 2 2 の公開鍵、伸張部 8 4 と相互認証する際に使用する共通鍵が記憶されている。これらのデータは、機器製造時に予め記憶されるデータである。また、外部メモリ 8 5 内に保持するコンテンツ鍵  $K_c$  および使用許諾条件情報の改竄チェック用のハッシュ値、必要に応じて決済用 ID、配送鍵  $K_d$ 、登録情報（の一部）（購入処理をしない場合、決済用 ID、配送鍵  $K_d$  は必要ない）は、機器を使用し始めてから記憶されるデータであり、これらのデータも記憶されている（購入処理を行う場合、課金情報も記憶される）。外部メモリ 8 5 には、暗号処理部 8 3 内にある機器個別の秘密鍵に対応する公開鍵の証明書、コンテンツ鍵  $K_c$  で暗号化されたコンテンツおよびその署名（この他に、必要に応じて個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_c$  およびその署名、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびその署名、必要に応じて取扱方針およびその署名、価格情報およびその署名も記憶される場合がある）、コンテンツを復号化する際に使用する保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_c$ 、そのコンテンツを利用する際の条件を示す使用許諾条件情報が記憶されている。また、必要に応じてコンテンツプロバイダ 2 の公開鍵証明書、サービスプロバイダ 3 の公開鍵証明書も記憶されている。

据置機器 5 2 には、ホームサーバ 5 1 の構成に加え、記録メディア 8 0 が備えられている。記録メディア 8 0 としては、通常の MD や CD-R の場合もあるし、電子配信専用の記憶メディアである場合もある。前者の場合、記憶されるデータはコピー禁止信号を付加された、復号化されたコンテンツになるが、勿論、暗

号化されたコンテンツを入れておいてもよい（保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ も併せて記憶しておいても良い。この時、再生できるのは記憶した機器のみになる。なぜなら、保存鍵 $K_{save}$ は機器毎に異なっているからである）。

また、記憶メディアとしては、図19が考えられる。電子配信専用記憶メディア120において、暗号処理部122内にある記憶モジュール125には、記録メディアの個別ID、記録メディア毎に異なる秘密鍵、この秘密鍵に対応する公開鍵の証明書（外部メモリ123に記録しておいても良い）、コンテンツ鍵 $K_{co}$ を暗号化するのに使用する保存鍵 $K_{save}$ （一般に、記憶メディア毎に異なる）、電子配信サービスセンタ1の公開鍵（センタとやりとりしない場合や外部メモリ123に電子配信サービスセンタ1の公開鍵証明書が有る場合には必要ない）、認証局の公開鍵、外部メモリ123の改竄を検査するためのハッシュ値、登録情報（の一部）が記憶されている。外部メモリ123には、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ（およびその署名）、保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報が記憶されており、必要に応じて取扱方針（およびその署名）、価格情報（およびその署名）、コンテンツプロバイダ2の公開鍵証明書、サービスプロバイダ3の公開鍵証明書が記憶されている。

図20、図21は、電子配信サービスセンタ1、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の間で送受信される情報を説明する図である。コンテンツプロバイダ2は、コンテンツプロバイダセキュアコンテナ（その詳細は後述する）にコンテンツプロバイダ2の公開鍵証明書（その詳細は後述する）を付して、サービスプロバイダ3に送信する。また、コンテンツプロバイダ2は、必要に応じて取扱方針およびその署名、コンテンツプロバイダ2の証明書を電子配信サービスセンタ1に送信する。

サービスプロバイダ3は、コンテンツプロバイダ2の公開鍵証明書を検証し、コンテンツプロバイダ2の公開鍵を入手し、受信したコンテンツプロバイダセキュアコンテナの署名を検証する（取扱方針のみ署名検証する場合もある）。署名の検証に成功した後、コンテンツプロバイダセキュアコンテナから取扱方針を取

り出し、これを基に価格情報を生成し、価格情報に署名を付けてサービスプロバイダセキュアコンテナとする（その詳細は後述する）。コンテンツプロバイダセキュアコンテナ、サービスプロバイダセキュアコンテナ、コンテンツプロバイダ2の公開鍵証明書、およびサービスプロバイダ3の公開鍵証明書（その詳細は後述する）をユーザホームネットワーク5に送信する。また、サービスプロバイダ3は、必要に応じて価格情報およびその署名、サービスプロバイダ3の公開鍵証明書を電子配信サービスセンタ1に送信する。

ユーザホームネットワーク5は、受信したセキュアコンテナを検証した後、セキュアコンテナの中に含まれる取扱方針および価格情報に基づいて購入処理を行い、課金情報を生成して暗号処理部内の記憶モジュールに保存し、使用許諾条件情報を生成し、コンテンツ鍵 $K_{co}$ を復号化して保存鍵 $K_{save}$ で再暗号化し、使用許諾条件情報および再暗号化されたコンテンツ鍵 $K_{co}$ を外部メモリ67に保存しておく。そして、使用許諾条件情報に沿って、コンテンツ鍵 $K_{co}$ を保存鍵 $K_{save}$ で復号化し、この鍵でコンテンツを復号化して利用する。課金情報は、所定のタイミングで一時鍵 $K_{temp}$ で暗号化され、署名が付され、必要に応じて取扱方針および価格情報と共に電子配信サービスセンタ1に送信される。

電子配信サービスセンタ1は、課金情報および価格情報を基に使用料金を算出し、また電子配信サービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3それぞれの利益を算出する。電子配信サービスセンタ1は、さらに、コンテンツプロバイダ2から受信した取扱方針、サービスプロバイダ3から受信した価格情報、必要に応じて取扱方針、並びにユーザホームネットワーク5から受信した取扱方針、価格情報を比較し、サービスプロバイダ3またはユーザホームネットワーク5で取扱方針の改竄または不正な価格の付加等の不正がなかったか否か等の監視をする。

更に、電子配信サービスセンタ1は、コンテンツプロバイダ2にコンテンツプロバイダの公開鍵証明書を送信し、サービスプロバイダ3にサービスプロバイダの公開鍵証明書を送信する。また、工場出荷時に、各機器に応じて作成した公開

鍵証明書を各機器に埋め込むため、各機器の公開鍵証明書に関するデータを工場に引き渡す。

図 2 2 は、コンテンツプロバイダセキュアコンテナを説明する図である。コンテンツプロバイダセキュアコンテナ 1 A は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツおよびその署名、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$  およびその署名、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびその署名、取扱方針および署名を含む。署名は、それぞれのデータにハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  を用いて生成されたデータである。なお、図 2 2 の場合は鍵データ（個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ ）に対してそれぞれ別々に署名を生成し付加するようにしたが、各鍵データ（個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ ）を 1 つにまとめて 1 つの署名を生成し付加するようにしても良い。このように常に一体で使用する鍵データを 1 つにまとめて 1 つの署名を付加することにより、署名の検証が 1 回で済む。

図 2 3 は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ 1 B は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツおよびその署名、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$  およびその署名、取扱方針および署名を含む。

図 2 4 は、コンテンツプロバイダセキュアコンテナの他の例を説明する図である。コンテンツプロバイダセキュアコンテナ 1 C は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、取扱方針、および署名を含む。署名は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  を用いて生成されたデータである。

図 2 5 は、コンテンツプロバイダセキュアコンテナの他の例を説明する図であ

る。コンテンツプロバイダセキュアコンテナ 1 D は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、取扱方針、および署名を含む。署名は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツ、個別鍵  $K_i$  で暗号化されたコンテンツ鍵  $K_{co}$ 、および取扱方針にハッシュ関数を適用して生成されたハッシュ値に、コンテンツプロバイダ 2 の秘密鍵  $K_{scp}$  を用いて生成されたデータである。

図 26 は、コンテンツプロバイダ 2 の公開鍵証明書を説明する図である。コンテンツプロバイダ 2 の公開鍵証明書 2 A は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、並びにコンテンツプロバイダ 2 の公開鍵  $K_{pcp}$  にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵  $K_{sca}$  を用いて生成したデータである。

図 27 は、コンテンツプロバイダ 2 の公開鍵証明書の他の例を説明する図である。コンテンツプロバイダ 2 の公開鍵証明書 2 B は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{pcp}$ 、並びに配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  に

ハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

図28は、コンテンツプロバイダ2の公開鍵証明書のまた別の例を説明する図である。コンテンツプロバイダ2の公開鍵証明書2Cは、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、個別鍵 $K_i$ の一部を配送鍵 $K_d$ で暗号化した、所定の種類のデータ、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、コンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ 、並びに個別鍵 $K_i$ の一部を配送鍵 $K_d$ で暗号化した、所定の種類のデータにハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵 $K_{sca}$ を用いて生成したデータである。

図29は、サービスプロバイダセキュアコンテナを説明する図である。サービスプロバイダセキュアコンテナ3Aは、価格情報および署名で構成されている。署名は、価格情報に対し必要に応じてハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ3の秘密鍵 $K_{ssp}$ を用いて生成されたデータである。

図30は、サービスプロバイダセキュアコンテナの他の例を説明する図である。サービスプロバイダセキュアコンテナ3Bは、コンテンツプロバイダセキュアコンテナ、価格情報、および署名を含む。署名は、コンテンツプロバイダセキュアコンテナ、および価格情報にハッシュ関数を適用して生成されたハッシュ値に、サービスプロバイダ3の秘密鍵 $K_{ssp}$ を用いて生成されたデータである。

図31は、サービスプロバイダ3の公開鍵証明書を説明する図である。サービスプロバイダ3の公開鍵証明書4Aは、公開鍵証明書のバージョン番号、認証局



がサービスプロバイダ 3 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ 3 の名前、サービスプロバイダ 3 の公開鍵  $K_{psp}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局がサービスプロバイダ 3 に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、サービスプロバイダ 3 の名前、並びにサービスプロバイダ 3 の公開鍵  $K_{psp}$  にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵  $K_{sca}$  を用いて生成したデータである。

図 3 2 は、U s e r 機器の公開鍵証明書を説明する図である。U s e r 機器の公開鍵証明書 5 A は、公開鍵証明書のバージョン番号、認証局が U s e r 機器（正確には暗号処理部（専用の I C チップ））に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、U s e r 機器の名前、U s e r 機器の公開鍵  $K_{pu}$ 、並びに署名を含む。署名は、公開鍵証明書のバージョン番号、認証局が U s e r 機器に対し割り付ける公開鍵証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、公開鍵証明書の有効期限、U s e r 機器の名前、並びに U s e r 機器の公開鍵  $K_{pu}$  にハッシュ関数を適用して生成されたハッシュ値に、認証局の秘密鍵  $K_{sca}$  を用いて生成したデータである。

図 3 3 および図 3 4 は取扱方針のデータフォーマットを示すものであり、当該取扱方針はコンテンツプロバイダ 2 によりシングルコンテンツ毎、またアルバムコンテンツ毎に生成され、ユーザホームネットワーク 5 が購入可能な利用権の内容を示す。

シングルコンテンツに対する取扱方針（図 3 3）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、コンテンツの I D、コンテンツプロバイダの I D、取扱方針の I D、取扱方針のバージョン、地域コード、使用可能機器条件、使用可能 U s e r 条件、サービスプロバイダの I D、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を

示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは、利用権毎に整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

また、アルバムコンテンツに対する取扱方針（図34）のデータには、データの種別、取扱方針の種類、取扱方針の有効期限、アルバムのID、取扱方針のバージョン、コンテンツプロバイダのID、取扱方針のID、地域コード、使用可能機器条件、使用可能User条件、サービスプロバイダのID、当該アルバムを構成するシングルコンテンツの取扱方針の数、そのシングルコンテンツの取扱方針の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの取扱方針のデータパケット、世代管理情報、当該取扱方針が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは、シングルコンテンツの取扱方針のルールと同様に、利用権毎に整理番号として付けられたルール番号、利用権内容番号、パラメータ、最低販売価格、コンテンツプロバイダの利益額、当該コンテンツプロバイダの利益率、データサイズ、送信情報から構成されている。

これら取扱方針において、データの種別はそのデータが取扱方針のデータであることを示し、取扱方針の種類は当該取扱方針がシングル又はアルバムコンテンツのいずれの取扱方針であるかを示している。取扱方針の有効期限は当該取扱方針の使用期間をその期限の切れる日付、又は使用を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのIDおよびアルバムのIDは取扱方針が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、コンテンツプロバイダのIDは、当該取扱方針を規定したコンテ

ンツプロバイダ 2 の I D を示している。

また、取扱方針の I D は当該取扱方針を識別するためのものであり、例えば、同一コンテンツに対して複数の取扱方針が設定された場合などに当該取扱方針を識別するために使用される。取扱方針のバージョンは使用期間に応じて改訂した取扱方針のその改訂情報を示している。従って、取扱方針はこれら取扱方針の I D および取扱方針のバージョンにより管理される。

地域コードは取扱方針の使用可能な地域をコード化して示しており、当該地域コードには取扱方針の使用可能な地域を限定する特定の地域を示すコードと、当該取扱方針を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は取扱方針を利用し得る機器の条件を示し、使用可能 U s e r 条件は取扱方針を利用し得るユーザの条件を示している。

サービスプロバイダの I D は取扱方針を利用するサービスプロバイダ 3 の I D を示しており、当該サービスプロバイダの I D には取扱方針を使用し得るサービスプロバイダ 3 を限定する特定のサービスプロバイダ 3 の I D と、当該取扱方針を複数（全て）のサービスプロバイダで使用し得るようにする I D とがある。

さらに、世代管理情報はコンテンツの再購入可能な最大回数を示す。署名は取扱方針から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

また、ルールにおいて、利用権内容番号は、利用権内容毎に付加された番号であり、パラメータは権利内容のパラメータを示す。最低販売価格は利用権内容に応じてシングルおよびアルバムコンテンツを販売する際の最低の販売価格を示し、コンテンツプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにコンテンツプロバイダ 2 が得ることのできる利益の金額および販売価格に対する利益率を示している。データサイズは送信情報のデータサイズを示し、当該送信情報は、コンテンツプロバイダ 2 が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利

用権の割引額でなるマイル情報や、必要に応じてコンテンツプロバイダ 2 が設定した各種情報からなる。

ここで、アルバムコンテンツの取扱方針において、複数のルールは、当該アルバムの購入形態を示している。また、アルバムコンテンツの取扱方針に格納された複数のシングルコンテンツの取扱方針において、当該取扱方針に格納されたルールは、それぞれ対応するシングルコンテンツがアルバムのなかから、シングル曲として単独で購入し得る、又は対応するシングルコンテンツがアルバム曲としてのみ購入し得る（すなわち、アルバムとして、他のシングルコンテンツと共に一体化してしか購入し得ない）等のようにアルバム内におけるシングルコンテンツの購入形態を示している。

従って、アルバムコンテンツの取扱方針においては、当該取扱方針のルールに基づいて、アルバムコンテンツを購入し、又はシングルコンテンツの取扱方針のルールに基づいて、シングルコンテンツをシングル曲として購入するように、アルバムコンテンツと、シングル曲として販売し得るシングルコンテンツとのいずれも選択して購入し得るように定義されている。

また、アルバムコンテンツの取扱方針においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この取扱方針に格納したシングルコンテンツの取扱方針の署名をそれぞれ検証しなくてもこのアルバムコンテンツの取扱方針と共に、各シングルコンテンツの取扱方針に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

因みに、シングルおよびアルバムコンテンツの取扱方針には、必要に応じて、コンテンツに対する署名の検証を実行するか否かを示す署名の検証の有無を格納し得る。これは、コンテンツのデータ量が比較的多く、署名の検証に時間がかかるためであり、取扱方針にかかる署名の検証の有無の情報が格納された場合には、当該情報に従ってコンテンツの署名の検証を実行し、又は当該検証を実行しないようにする。

また、アルバムコンテンツの取扱方針においては、当該アルバムを構成する複

数のシングルコンテンツの取扱方針を格納しているものの、これら複数のシングルコンテンツの取扱方針を格納しなくても良い。

さらに、シングルおよびアルバムコンテンツの取扱方針においては、コンテンツプロバイダの利益額および利益率を電子配信サービスセンタ 1 により一括管理しても良いため、図 3 5 および図 3 6 に示すように、これらコンテンツプロバイダの利益額および利益率を除いて構成しても良い。

図 3 7 および図 3 8 は価格情報のデータフォーマットを示すものであり、当該価格情報はサービスプロバイダ 3 において、コンテンツプロバイダ 2 から与えられるシングルコンテンツの取扱方針毎、またアルバムコンテンツの取扱方針毎に生成され、シングルコンテンツおよびアルバムコンテンツの価格を示す。

シングルコンテンツに対する価格情報（図 3 7）のデータには、データの種別、価格情報の種類、価格情報の有効期限、コンテンツの ID、サービスプロバイダの ID、価格情報の ID、価格情報のバージョン、地域コード、使用可能機器条件、使用可能 User 条件、コンテンツプロバイダの ID、当該価格情報が付加された取扱方針の ID、当該価格情報が示す購入可能な利用権を含むルールの数、当該ルールの格納位置を示すアドレス情報、そのアドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

また、アルバムコンテンツに対する価格情報（図 3 8）のデータには、データの種別、価格情報の種類、価格情報の有効期限、アルバムの ID、サービスプロバイダの ID、価格情報の ID、価格情報のバージョン、地域コード、使用可能機器条件、使用可能 User 条件、コンテンツプロバイダの ID、当該価格情報が付加された取扱方針の ID、当該アルバムを構成するシングルコンテンツの価格情報の数、そのシングルコンテンツの価格情報の格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたシングルコンテンツの価格情報のデ

ータパッケージ、当該価格情報が示す購入可能な利用権を含むルールの数、そのルールの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納されたルール、公開鍵証明書、署名が格納されている。

そして、ルールは、シングルコンテンツに対する価格情報のルールと同様に、利用権毎に整理番号として付けられたルール番号、サービスプロバイダの利益額、当該サービスプロバイダの利益率、価格、データサイズ、送信情報から構成されている。

これら価格情報において、データの種別はこのデータが価格情報のデータであることを示し、価格情報の種類は当該価格情報がシングルコンテンツ又はアルバムコンテンツのいずれの価格情報であるかを示している。価格情報の有効期限は当該価格情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。コンテンツのIDおよびアルバムのIDは価格情報が示す購入可能なシングルコンテンツおよびアルバムコンテンツを示し、サービスプロバイダのIDは当該価格情報を作成したサービスプロバイダ3のIDを示している。

また、価格情報のIDは当該価格情報を識別するためのものであり、例えば、同一コンテンツに対して複数の価格情報が設定された場合などに当該価格情報を識別するために使用される。価格情報のバージョンは使用期間に応じて改訂された価格情報の改訂情報を示している。従って、価格情報はこれら価格情報のIDおよび価格情報のバージョンにより管理される。

地域コードは価格情報の使用可能な地域をコード化して示しており、当該地域コードには価格情報の使用可能な地域を限定する特定の地域を示すコードと、当該価格情報を全ての地域で使用可能にするコードを割り当てることができる。使用可能機器条件は価格情報を利用し得る機器の条件を示し、使用可能User条件は価格情報を利用し得るユーザの条件を示している。コンテンツプロバイダのIDは価格情報を付加した取扱方針を規定したコンテンツプロバイダ2のIDを示している。取扱方針のIDは価格情報を付加した取扱方針を識別するためのもの

のである。

さらに、署名は価格情報から当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

また、ルールにおいて、ルール番号は対応する取扱方針が示すルールのルール番号をそのまま用いる。サービスプロバイダの利益額および利益率はシングルコンテンツおよびアルバムコンテンツが購入されたときにサービスプロバイダ3が得ることのできる利益の金額および価格に対する利益率を示し、価格はサービスプロバイダ3により利用権内容および対応する最低販売価格に基づいて設定されたシングルコンテンツおよびアルバムコンテンツの販売価格を示す。データサイズは送信情報のデータサイズを示し、当該送信情報は、サービスプロバイダ3が設定した、利用権の購入によりユーザに加算されるポイントや、当該ポイントに応じた利用権の割引額となるマイル情報や、必要に応じてサービスプロバイダ3が設定した各種情報からなる。

ここで、サービスプロバイダ3は、価格情報を生成する際、対応する取扱方針が示す購入可能な全ての利用権を当該価格情報が示す購入可能な利用権として設定することができると共に、当該取扱方針が示す購入可能な全ての利用権のうちから任意に選定した利用権を価格情報が示す購入可能な利用権として設定することもでき、コンテンツプロバイダ2が規定した利用権を選定し得る。

また、アルバムコンテンツの価格情報において、複数のルールは、アルバムの購入形態に応じた販売価格を規定している。また、アルバムコンテンツの価格情報に格納された複数のシングルコンテンツの価格情報のうち、シングル曲として販売し得るシングルコンテンツの価格情報のルールは、当該シングル曲として販売し得るシングルコンテンツの販売価格を規定している。

従って、アルバムコンテンツの価格情報においては、当該価格情報1つでアルバムの販売価格と、シングル曲として販売し得るシングルコンテンツの販売価格

とを認識し得るようになされている。

また、アルバムコンテンツの価格情報においては、全体に対して署名を付けたことにより、当該署名を検証するだけで、この価格情報に格納したシングルコンテンツの価格情報の署名をそれぞれ検証しなくてもこのアルバムコンテンツの価格情報と共に、各シングルコンテンツの価格情報に対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

因みに、シングルおよびアルバムの価格情報においては、図 3 3 および図 3 4 について上述した取扱方針と同様にコンテンツに対する署名の検証の有無を格納し得る。また、アルバムコンテンツの価格情報においては、当該アルバムを構成する複数のシングルコンテンツの価格情報を格納しているものの、これら複数のシングルコンテンツの価格情報を格納しなくても良い。

さらに、シングルおよびアルバムコンテンツの価格情報においては、サービスプロバイダの利益額および利益率を電子配信サービスセンタ 1 により一括管理しても良いため、図 3 9 および図 4 0 に示すように、これらサービスプロバイダの利益額および利益率を除いて構成しても良い。

図 4 1 は使用許諾条件情報のデータフォーマットを示すものであり、当該使用許諾条件情報はユーザホームネットワーク 5 内の機器において、ユーザがコンテンツを購入した際、当該購入したコンテンツの取扱方針に基づいて作成され、この取扱方針の示す利用権内容のうちのユーザが選択した利用権内容を示す。

使用許諾条件情報のデータには、データの種別、使用許諾条件情報の種類、使用許諾条件情報の有効期限、コンテンツの ID、アルバムの ID、暗号処理部の ID、ユーザの ID、コンテンツプロバイダの ID、取扱方針の ID、取扱方針のバージョン、サービスプロバイダの ID、価格情報の ID、価格情報のバージョン、使用許諾条件情報の ID、再生権（利用権）に整理番号として付けられたルール番号、利用権内容番号、再生残り回数、再生権の有効期限、複製権（利用権）に整理番号として付けられたルール番号、利用権内容番号、複製の残り回数、世代管理情報、再生権を保有する暗号処理部の ID が格納されている。



使用許諾条件情報において、データの種別はこのデータが使用許諾条件情報のデータであることを示し、使用許諾条件情報の種類は当該使用許諾条件情報がシングルコンテンツ又はアルバムコンテンツのいずれの使用許諾条件情報であることを示している。使用許諾条件情報の有効期限は当該使用許諾条件情報の使用期間をその期限の切れる日付、又は使用開始の基準となる日から期限の切れる日までの日数などによって示している。

コンテンツのIDには購入されたシングルコンテンツを示すIDが記述され、アルバムのIDにはアルバムが購入されたときのみ当該アルバムを示すIDが記述される。実際には、コンテンツがシングルとして購入された場合、コンテンツのIDのみに購入されたシングルコンテンツを示すIDが記述され、また、コンテンツがアルバムとして購入された場合には、コンテンツのIDに、アルバムを構成する全てのシングルコンテンツのIDが記述され、かつアルバムのIDに購入されたアルバムを示すIDが記述される。従って、このアルバムのIDをみれば、購入されたコンテンツがシングルであるか、又はアルバムであるかを容易に判断し得る。

暗号処理部のIDはコンテンツを購入処理したユーザホームネットワーク5内の機器の暗号処理部を示す。ユーザのIDはコンテンツを購入したユーザホームネットワーク5内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示している。

また、コンテンツプロバイダのIDは使用許諾条件情報を作成するために用いた取扱方針を規定したコンテンツプロバイダ2のIDを示し、取扱方針のIDは当該使用許諾条件情報を作成するために用いた取扱方針を示す。取扱方針のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。サービスプロバイダのIDは使用許諾条件情報を作成するために用いた価格情報を作成したサービスプロバイダ3のIDを示し、価格情報のIDは当該使用許諾条件情報を作成するために用いた価格情報を示す。価格情報のバージョンは使用許諾条件情報を作成するために用いた取扱方針の改訂情報を示している。

従って、これらコンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、サービスプロバイダのID、価格情報のIDおよび価格情報のバージョンにより、ユーザが購入したコンテンツを提供したコンテンツプロバイダ2又はサービスプロバイダ3を知り得るようになされている。

使用許諾条件情報のIDはコンテンツを購入したユーザホームネットワーク5内の機器の暗号処理部が付けるものであり、当該使用許諾条件情報を識別するために使用される。再生権のルール番号は利用権のうちの再生権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する再生権の内容を示す。再生残り回数は購入したコンテンツに対して予め設定された再生回数のうちの残りの再生回数を示し、再生権の有効期限は購入したコンテンツの対する再生可能期間をその期限の切れる日時などによって示している。

また、複製権のルール番号は利用権のうちの複製権に付けられた整理番号を示し、対応する取扱方針および価格情報が示すルールのルール番号をそのまま用いる。利用権内容は後述する複製権の内容を示す。複製残り回数は購入したコンテンツに対して予め設定された複製回数のうちの残りの複製回数を示す。

さらに、世代管理情報はコンテンツを再購入した際に当該コンテンツの再購入可能な残り回数を示す。再生権を保有する暗号処理部のIDは現時点において再生権を保有する暗号処理部を示しており、管理移動したときには再生権を保有する暗号処理部のIDが変更される。

因みに、使用許諾条件情報においては、複製権に対して有効期限を規定しても良く、当該有効期限を規定した場合には購入したコンテンツに対する複製可能期間をその期限の切れる日時などによって示す。

図42は課金情報を示すものであり、当該課金情報はユーザホームネットワーク5内の機器により、コンテンツの購入の際に、当該コンテンツに対応する取扱方針および価格情報に基づいて生成される。

課金情報のデータには、データの種別、暗号処理部のID、ユーザのID、コ

コンテンツのID、コンテンツプロバイダのID、取扱方針のID、取扱方針のバージョン、サービスプロバイダのID、価格情報のID、価格情報のバージョン、使用許諾条件情報のID、ルール番号、コンテンツプロバイダ2の利益額および利益率、サービスプロバイダの利益額および利益率、世代管理情報、コンテンツプロバイダの設定した送信情報のデータサイズ、そのコンテンツプロバイダの設定した送信情報、サービスプロバイダの設定した送信情報のデータサイズ、そのサービスプロバイダの設定した送信情報、供給元のIDが格納されている。

課金情報において、データの種別は当該データが課金情報であることを示し、暗号処理部のIDは、コンテンツの購入処理を実行して当該課金情報を生成した機器の暗号処理部を示す。ユーザのIDはコンテンツを購入したユーザホームネットワーク5内の機器を複数のユーザが共有しているときに、当該機器を共有する複数のユーザを示し、コンテンツのIDは当該購入されたコンテンツ（シングルコンテンツ又はアルバムコンテンツ）を示す。

また、コンテンツプロバイダのIDは購入処理に用いた取扱方針を規定したコンテンツプロバイダ2のID（この取扱方針に含まれるコンテンツプロバイダのID）を示し、取扱方針のIDは当該購入処理に用いた取扱方針を示す。取扱方針のバージョンは、購入処理に用いた取扱方針の改訂情報を示す。サービスプロバイダのIDは購入処理に用いた価格情報を作成したサービスプロバイダ3のID（この価格情報に含まれるサービスプロバイダのID）を示し、価格情報のIDは当該購入処理に用いた価格情報を示す。価格情報のバージョンは、購入処理に用いた価格情報の改訂情報を示す。

使用許諾条件情報のIDは購入処理の際に作成した使用許諾条件情報のIDを示し、ルール番号は購入された利用権に整理番号として付けられたルール番号を示す。コンテンツプロバイダの利益額および利益率はコンテンツの購入によりコンテンツプロバイダ2に分配される配当の金額および売上に対する割合を示し、サービスプロバイダの利益額および利益率は当該コンテンツの購入によりサービスプロバイダ3に分配される配当の金額および売上に対する割合を示す。

さらに、世代管理情報は購入されたコンテンツの世代を示す。また、コンテンツプロバイダの設定した送信情報のデータサイズおよびそのコンテンツプロバイダの設定した送信情報には、購入処理に用いた取扱方針が示すデータサイズと、送信情報をそのまま格納すると共に、サービスプロバイダの設定した送信情報のデータサイズおよびそのサービスプロバイダの設定した送信情報には購入処理に用いた価格情報が示すデータサイズと、送信情報をそのまま格納する。そして、供給元のIDは、購入処理したコンテンツの供給元の機器を示し、このIDはコンテンツの再購入が行われる毎に累積される。

因みに、課金情報においては、コンテンツプロバイダの利益額および利益率と、サービスプロバイダの利益額および利益率を電子配信サービスセンタ1により一括管理しても良いため、図43に示すように、これらコンテンツプロバイダの利益額および利益率およびサービスプロバイダの利益額および利益率を除いて構成しても良い。

図44は購入可能な利用権の内容を示したものであり、当該利用権としては、大きく分けて再生権、複製権、権利内容変更権、再購入権、追加購入権、管理移動権がある。

再生権には、期間制限および回数制限のない無制限再生権と、再生期間を制限する期間制限付き再生権、再生の積算時間を制限する積算時間制限付き再生権、再生回数を制限する回数制限付き再生権がある。複製権には、期間制限、回数制限およびコピー管理情報（例えば、シリアルコピーマネージメント：SCMS）のないコピー管理情報なし無制限複製権、複製回数を制限するもののコピー管理情報のない回数制限付きおよびコピー管理情報なし複製権、期間制限および回数制限はないもののコピー管理情報を付加して提供するコピー管理情報付き複製権、複製回数を制限し、かつコピー管理情報を付加して提供する回数制限およびコピー管理情報付き複製権がある。因みに、複製権としては、この他に複製可能期間を制限する期間制限付き複製権（コピー管理情報を付加するものと、当該コピー管理情報を付加しないものとがある）や、複製の積算時間（すなわち、複製さ

れたコンテンツの再生に要する積算時間)を制限する積算時間制限付き複製権(コピー管理情報を付加するものと、当該コピー管理情報を付加しないものがある)等がある。

また、権利内容変更権は上述したように既に購入した利用権の内容を別の内容に変更する権利であり、再購入権も上述したように他の機器で購入した権利に基づき利用権を別途購入する権利である。追加購入権は、既に単独で購入したコンテンツに当該コンテンツを含むアルバムの他のコンテンツを追加購入してアルバム化する権利であり、管理移動権は購入した利用権を移動して保有者を変更する権利である。

次に、図33などに示されている利用権内容の具体例を説明する。実際に、無制限再生権のデータとしては、図45(A)に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。期間制限付き再生権のデータとしては、図45(B)に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報が利用権内容の領域に格納される。

積算時間制限付き再生権のデータとしては、図45(C)に示すように再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る積算時間の制限を示す日数および時間の情報とが利用権内容の領域に格納される。回数制限付き再生権のデータとしては、図45(D)に示すように、再生権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再生権の有効期限の情報と、再生し得る回数を示す再生回数の情報とが利用権内容の領域に格納される。

また、コピー管理情報なし無制限複製権のデータとしては、図45(E)に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準

となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限付きおよびコピー管理情報なし複製権のデータとしては、図45(F)に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

コピー管理情報付き複製権のデータとしては、図45(G)に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報が利用権内容の領域に格納されている。回数制限およびコピー管理情報付き複製権のデータとしては、図45(H)に示すように、複製権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該複製権の有効期限の情報と、複製し得る回数を示す複製回数の情報とが利用権内容の領域に格納される。

さらに、権利内容変更権のデータとしては、図45(I)に示すように、当該権利内容変更権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該権利内容変更権の有効期限の情報と、変更前の利用権内容を検索するための旧ルール番号と、変更後の利用権内容を検索するための新ルール番号とが利用権内容の領域に格納される。因みに、利用権内容として、例えば、期間制限付き再生権1つをみても、その期間の設定により複数種類の期間制限付き再生権が存在するように、利用権内容毎に複数種類の内容が存在する。従って、利用権内容を利用権内容番号だけでは管理し難いため、権利内容変更権においては、これら利用権内容毎の複数の内容毎に付けられたルール番号により利用権内容を管理する。

再購入権のデータとしては、図45(J)に示すように、当該再購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該再購入権の有効期限の情報と、再購入前の

利用権内容を検索するための旧ルール番号と、再購入後の利用権内容を検索するための新ルール番号と、再購入し得る最大回数の示す最大配信世代情報とが利用権内容の領域に格納される。

追加購入権のデータとしては、図 4 5 (K) に示すように、当該追加購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該追加購入権の有効期限の情報と、アルバムコンテンツを構成する複数のシングルコンテンツのうちの既に購入したシングルのコンテンツを示す最小保有コンテンツ数および最大保有コンテンツ数とが利用権内容の領域に格納される。

管理移動権のデータとしては、図 4 5 (L) に示すように、当該管理移動権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該管理移動権の有効期限の情報が利用権内容の領域に格納される。

因みに、かかる利用権内容として、例えば、ゲームのデータを複数のコンテンツに分割した際にこれらコンテンツを所定の順番に従って購入するためのコンテンツ購入権を規定しても良い。そして、コンテンツ購入権のデータとしては、図 4 5 (M) に示すように、当該コンテンツ購入権の有効期間をその期限の切れる日付、又は有効期間開始の基準となる日から期限の切れる日までの日数などによって示す当該コンテンツ購入権の有効期限の情報と、既に購入されているコンテンツの ID と、既に購入された利用権内容を検索するための旧ルール番号と、新たに購入する利用権内容を検索するための新ルール番号とを利用権内容の領域に格納する。このようにすることで、連続したストーリーをもつゲームプログラムなどを、ユーザに連続して購入させるようにしたり、また、コンテンツ（ゲーム）そのものをアップグレードし得る。

図 4 6 はシングルコンテンツのデータフォーマットを示すものであり、当該シングルコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、コンテンツのカテゴリー、コンテンツの ID、コンテンツプロバイ

ダのID、コンテンツの暗号方式、暗号化したコンテンツのデータ長、その暗号化したコンテンツ、公開鍵証明書、署名が格納されている。

このシングルコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがシングルであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示している。コンテンツのカテゴリーは当該コンテンツが音楽データ、プログラムデータ、映像データなどのいずれのカテゴリーのものであるかを示し、コンテンツのIDはこのシングルコンテンツを識別するためのものである。

コンテンツプロバイダのIDは、このシングルコンテンツを保有するコンテンツプロバイダ2のIDを示す。コンテンツの暗号方式は当該コンテンツの暗号に用いる暗号方式（例えば、DES）を示す。署名はシングルコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

また、図47はアルバムコンテンツのデータフォーマットを示すものであり、当該アルバムコンテンツのデータには、データの種別、コンテンツの種類、コンテンツの有効期限、アルバムのID、コンテンツプロバイダのID、シングルコンテンツの数、シングルコンテンツのアドレス情報、シングルコンテンツ、公開鍵証明書、署名が格納されている。

このアルバムコンテンツにおいて、データの種別はそのデータがコンテンツのデータであることを示し、コンテンツの種類は当該コンテンツがアルバムであることを示す。コンテンツの有効期限は当該コンテンツの配信期限をこの期限の切れる日付、又は配信を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのIDはこのアルバムコンテンツを識別するためのものである。

コンテンツプロバイダのIDは、このアルバムコンテンツを保有するコンテン



ツプロバイダ 2 の ID を示す。シングルコンテンツの数はアルバムを構成するシングルコンテンツの数を示し、シングルコンテンツのアドレス情報は当該アルバムを構成するシングルコンテンツの格納位置を示し、そして、シングルコンテンツは当該アドレス情報の示す位置に実際に格納された、このアルバムを構成する複数のシングルコンテンツのデータパケットである。また、署名はアルバムコンテンツのデータから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

そして、アルバムコンテンツにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、このアルバムコンテンツに格納したシングルコンテンツの署名をそれぞれ検証しなくても当該アルバムコンテンツと共に、各シングルコンテンツに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

図 48 はシングルコンテンツ用の鍵のデータフォーマットを示すものであり、当該シングルコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、コンテンツの ID、コンテンツプロバイダの ID、鍵のバージョン、コンテンツ鍵  $K_{\infty}$  の暗号方式、暗号化されたコンテンツ鍵  $K_{\infty}$ 、個別鍵  $K_i$  の暗号方式、暗号化された個別鍵  $K_i$ 、公開鍵証明書、署名が格納されている。

シングルコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがシングルコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵  $K_{\infty}$  および個別鍵  $K_i$ ）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、コンテンツの ID はコンテンツ鍵  $K_{\infty}$  により暗号化するシングルコンテンツを示す。コンテンツプロバイダの ID はコンテンツを保有し、かつコンテンツ鍵  $K_{\infty}$  を生成したコンテンツプロバイダ 2 の ID を示す。

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵  $K_{\infty}$  および個

別鍵 $K_i$ )の改訂情報を示す。コンテンツ鍵 $K_{co}$ の暗号方式は個別鍵 $K_i$ を用いてコンテンツ鍵 $K_{co}$ を暗号化する際の暗号方式(例えば、DES)を示し、暗号化されたコンテンツ鍵 $K_{co}$ はその暗号方式により個別鍵 $K_i$ を用いて暗号化されたコンテンツ鍵 $K_{co}$ を示す。個別鍵 $K_i$ の暗号化方式は配送鍵 $K_d$ を用いて個別鍵 $K_i$ を暗号化する際の暗号方式(例えば、Triple-DES-CBC)を示し、暗号化された個別鍵 $K_i$ はその暗号方式により配送鍵 $K_d$ を用いて暗号化された個別鍵 $K_i$ を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵は公開鍵証明書に含まれている。

ここで、配送鍵 $K_d$ および個別鍵 $K_i$ はコンテンツプロバイダ2からシングルコンテンツ用の鍵データにより常に一体にされて配送される。そして、シングルコンテンツ用の鍵データにおいては、その全体に対して1つの署名が付加されている。従って、シングルコンテンツ用の鍵データを受け取った機器においては、暗号化されたコンテンツ鍵 $K_{co}$ および暗号化された個別鍵 $K_i$ に対してそれぞれ別々に署名を検証する必要がなく、シングルコンテンツ用の鍵データの1つの署名を検証するだけで当該暗号化されたコンテンツ鍵 $K_{co}$ および暗号化された個別鍵 $K_i$ に対する署名の検証をしたことになり、かくして、これら暗号化されたコンテンツ鍵 $K_{co}$ および暗号化された個別鍵 $K_i$ に対する署名の検証を簡易化し得る。

因みに、個別鍵 $K_i$ は、当該個別鍵 $K_i$ を用いてコンテンツ鍵 $K_{co}$ を暗号化するコンテンツプロバイダのIDと共に暗号化される。実際に、トリプルDESのCBCモードと呼ばれる暗号化方式によってコンテンツプロバイダのIDと共に個別鍵 $K_i$ を暗号化する方法を図49を用いて説明する。すなわち、かかる暗号化方式では、所定の初期値と、個別鍵 $K_i$ (64bit)とを接続した後、配送鍵 $K_d$ を用いてトリプルDESのCBCモードによる暗号化方式で暗号化し、この結果、得られた64bitの第1の値をコンテンツプロバイダのID(64bit

）と接続した後、再び配送鍵 $K_d$ を用いてトリプルデスのCBCモードによる暗号化方式で暗号化し、かくして、64 bitの第2の値を得る。そして、かかる暗号化方式では、第1の値と第2の値とを接続した16バイトのデータが、シングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$ となる（この場合、第1の値はシングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$ の始めの64 bitのデータに相当し、また、第2の値は当該シングルコンテンツ用の鍵データに格納される暗号化された個別鍵 $K_i$ 内の第1の値に続く64 bitのデータとなる）。

また、図50はアルバムコンテンツ用の鍵データを示すものであり、当該アルバムコンテンツ用の鍵データには、データの種別、鍵データの種類、鍵の有効期限、アルバムのID、コンテンツプロバイダのID、鍵のバージョン、アルバムを構成するシングルコンテンツの暗号化の際に用いるシングルコンテンツ用の鍵データの数、その鍵データの格納位置を示すアドレス情報、当該アドレス情報の示す位置に格納された鍵データパケット、公開鍵証明書、署名が格納されている。

。アルバムコンテンツ用の鍵データにおいて、データの種別はこのデータが鍵のデータであることを示し、鍵データの種類は当該鍵データがアルバムコンテンツ用であることを示す。鍵の有効期限は鍵データに示す鍵（コンテンツ鍵 $K_c$ ）の使用期間をその期限の切れる日付、又は鍵の使用を開始した基準となる日から期限の切れる日までの日数などによって示し、アルバムのIDはコンテンツ鍵 $K_c$ により暗号化するシングルコンテンツからなるアルバムコンテンツを示す。コンテンツプロバイダのIDはアルバムコンテンツを暗号化するコンテンツプロバイダ2のIDを示す。

鍵のバージョンは使用期間に応じて改訂された鍵（コンテンツ鍵 $K_c$ ）の改訂情報を示す。署名はシングルコンテンツ用の鍵データから当該署名を除く、データの種別から公開鍵証明書までの全体に対して付けられるものである。署名を作成する際に用いたアルゴリズムおよびパラメータと、当該署名の検証に用いる鍵

は公開鍵証明書に含まれている。

そして、アルバムコンテンツ用の鍵データにおいては、全体に対して署名を付けたことにより、当該署名を検証するだけで、当該アルバムコンテンツ用の鍵データに格納した複数のシングルコンテンツ用の鍵データの署名をそれぞれ検証しなくても当該アルバムコンテンツ用の鍵データと共に、各シングルコンテンツ用の鍵データに対しても合わせて改竄のチェックなどを行うことができ、かくして署名の検証を簡易化し得る。

図51は、1つの共通鍵で、共通鍵暗号であるDESを用いる、暗号処理部65と伸張部66との相互認証の動作を説明する図である。図51において、Aを伸張部66、Bを暗号処理部65とすると、暗号処理部65は64ビットの乱数 $R_B$ を生成し、 $R_B$ および自己のIDである $ID_B$ を、上位コントローラ62を介して伸張部66に送信する。これを受信した伸張部66は、新たに64ビットの乱数 $R_A$ を生成し、 $R_A$ 、 $R_B$ 、 $ID_B$ をDESのCBCモードで鍵 $K_{AB}$ を用いて暗号化し、上位コントローラ62を介して暗号処理部65に返送する。

DESのCBCモードとは、暗号化する際に、一つ前の出力と入力を排他的論理和し、それから暗号化する手法である。本例で言うならば、

$$X = \text{DES}(K_{AB}, R_A + IV) \quad IV = \text{初期値、} + : \text{排他的論理和}$$

$$Y = \text{DES}(K_{AB}, R_B + X)$$

$$Z = \text{DES}(K_{AB}, ID_B + Y)$$

となり、出力は、X、Y、Zとなる。これらの式において、 $\text{DES}(K_{AB}, R_A + IV)$ は鍵 $K_{AB}$ を使ってデータ $R_A + IV$ をDESで暗号化することを表し、 $\text{DES}(K_{AB}, R_B + X)$ は鍵 $K_{AB}$ を使ってデータ $R_B + X$ をDESで暗号化することを表し、 $\text{DES}(K_{AB}, ID_B + Y)$ は鍵 $K_{AB}$ を使ってデータ $ID_B + Y$ をDESで暗号化することを表す。

これを受信した暗号処理部65は、受信データを鍵 $K_{AB}$ で復号化し、 $R_B$ および $ID_B$ が、暗号処理部65が送信したものと一致するか検査する。この検査に通った場合、伸張部66を正当なものとして認証する。続けて、セッション鍵（

一時鍵 $K_{temp}$ のこと、乱数により生成する)  $SK_{AB}$ を生成し、 $R_B$ 、 $R_A$ 、 $SK_{AB}$ をDESのCBCモードで鍵 $K_{AB}$ を用いて暗号化し、上位コントローラ62を介して伸張部66に送信する。これを受信した伸張部66は、受信データを鍵 $K_{AB}$ で復号化し、 $R_B$ および $R_A$ が、伸張部66が送信したものと一致するか検査する。この検査に通った場合、暗号処理部65を正当なものとして認証し、データ $SK_{AB}$ をセッション鍵として以降の通信に使用する。なお、受信データの検査の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

図52は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、ホームサーバ51の暗号処理部65内の相互認証モジュール95と据置機器52の暗号処理部73内の図示せぬ相互認証モジュールとの相互認証の動作を説明する図である。図52において、Aを暗号処理部73、Bを暗号処理部65とすると、暗号処理部65は、64ビットの乱数 $R_B$ を生成し、上位コントローラ62、通信部61を介して据置機器52へ送信する。これを受信した据置機器52は、暗号処理部73において新たに64ビットの乱数 $R_A$ 、および標数 $p$ より小さい乱数 $A_K$ を生成する。そして、ベースポイント $G$ を $A_K$ 倍した点 $A_V$ を求め、 $R_A$ 、 $R_B$ 、 $A_V$  (X座標とY座標)を接続し(64ビット+64ビット+160ビット+160ビットで、448ビットになる)、そのデータに対し、自己の持つ秘密鍵で署名データ $A.Sig$ を生成する。なお、ベースポイントのスカラー倍は図10の署名の生成で説明した方法と同じであるためその説明は省略する。データの接続とは、例えば次のようになる。16ビットのデータAと16ビットのデータBを接続すると、上位16ビットのデータがAで、下位16ビットのデータがBになる32ビットのデータのことを言う。署名の生成は図10の署名の生成で説明した方法と同じであるためその説明は省略する。

次に、暗号処理部73は、 $R_A$ 、 $R_B$ 、 $A_V$ および署名データ $A.Sig$ を上位コントローラ72に引き渡し、上位コントローラ72は、据置機器52用の公開鍵証明書(小容量記憶部75に保存されている)を追加して通信部71を介し

てホームサーバ51に送信する。公開鍵証明書は図32で説明しているのでその詳細は省略する。これを受信したホームサーバ51は、暗号処理部65において据置機器52の公開鍵証明書の署名を検証する。署名の検証は、図11の署名の検証で説明した方法と同じであるためその説明は省略する。次に、送られてきたデータのうち、乱数 $R_B$ が、暗号処理部65が送信したものと同一かどうか検査し、同一であった場合には署名データ $A.Sig$ を検証する。検証に成功したとき、暗号処理部65は暗号処理部73を認証する。なお、署名の検証は図11の署名の検証で説明した方法と同じであるためその説明は省略する。そして、暗号処理部65は、標数 $p$ より小さい乱数 $B_K$ を生成し、ベースポイント $G$ を $B_K$ 倍した点 $B_V$ を求め、 $R_B$ 、 $R_A$ 、 $B_V$ （ $X$ 座標と $Y$ 座標）を接続し、そのデータに対し、自己の持つ秘密鍵で署名データ $B.Sig$ を生成する。最後に、暗号処理部65は、 $R_B$ 、 $R_A$ 、 $B_V$ および署名データ $B.Sig$ を上位コントローラ62に引き渡し、上位コントローラ62は、ホームサーバ51用の公開鍵証明書（大容量記憶部68に保存されている）を追加して通信部61を介して据置機器52に送信する。

これを受信した据置機器52は、暗号処理部73においてホームサーバ51の公開鍵証明書の署名を検証する。次に、送られてきたデータのうち、乱数 $R_A$ が、暗号処理部73が送信したものと同一かどうか検査し、同一であった場合には署名データ $B.Sig$ を検証する。検証に成功したとき、暗号処理部73は暗号処理部65を認証する。

両者が認証に成功した場合には、暗号処理部65は $B_K A_V$ （ $B_K$ は乱数だが、 $A_V$ は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、暗号処理部73は $A_K B_V$ を計算し、これら点の $X$ 座標の下位64ビットをセッション鍵（一時鍵 $K_{temp}$ ）として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。因に、通信に使用するセッション鍵としては、 $X$ 座標の下位64ビットに限らず、 $Y$ 座標の下位64ビットを用いるようにしても良い。なお、相互認証後の秘密通信においては、データは一時鍵

$K_{temp}$  で暗号化されるだけでなく、その暗号化された送信データに署名が付されることがある。

署名の検証、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

図 5 3 は、ユーザホームネットワーク 5 内の決済可能機器が、電子配信サービスセンタ 1 へ課金情報を送信するときの動作を説明する図である。ユーザホームネットワーク 5 内の決済可能機器は、登録情報から代理決済すべき対象機器を検索し、相互認証を行い、課金情報を共有した一時鍵  $K_{temp}$  (この鍵は、相互認証するたびに異なる) で暗号化して送らせる (このとき、データに署名が付いている)。全ての機器について処理が終わった後、電子配信サービスセンタ 1 と相互認証をし、共有した一時鍵で全ての課金情報を暗号化し、これらに署名データを付け、登録情報、必要に応じて取扱方針、価格情報と共に電子配信サービスセンタ 1 に送信する。なお、ユーザホームネットワーク 5 から電子配信サービスセンタ 1 へ送信される課金情報に、取扱方針の ID や価格情報の ID 等の金額の分配に必要な情報が含まれていることにより、情報量の多い取扱方針や価格情報は必ずしも送信する必要はない。ユーザ管理部 1 8 はこれを受信する。ユーザ管理部 1 8 は、受信した課金情報、登録情報、取扱方針、および価格情報に対する署名データの検証を行う。署名の検証は図 1 1 で説明した方法と同じなため詳細は省略する。次に、ユーザ管理部 1 8 は、相互認証のときに共有した一時鍵  $K_{temp}$  で課金情報を復号化し、取扱方針、および価格情報と共に経歴データ管理部 1 5 に送信する。

因みに、この実施の形態においては、相互認証後に送信されるデータは必要に応じて一時鍵  $K_{temp}$  で暗号化される。例えばコンテンツ鍵  $K_c$  や配送鍵  $K_d$  は内容が見られてしまうとデータを不正に利用されてしまうため一時鍵  $K_{temp}$  で暗号化して外部から見えないようにする必要がある。これに対して課金情報や使用許諾条件情報等は内容が見られても、データを不正に利用することができないため、必ずしも一時鍵  $K_{temp}$  で暗号化する必要はないが、例えば課金情報の金額が改

竄されたり使用許諾条件情報の使用条件が緩くなるように改竄されると金額の授受に関係する当事者に損害が発生することになる。従って、課金情報や使用許諾条件情報には署名を付して送信することにより改竄を防止している。ただし、コンテンツ鍵 $K_c$ や配送鍵 $K_d$ を送信する場合にも署名を付けても良い。

そして、送信側では送られるデータに対して、又は送られるデータを一時鍵 $K_{temp}$ で暗号化したデータに対して署名を生成し、データ及び署名を送信する。受信側では、送られたデータが一時鍵 $K_{temp}$ で暗号化されていない場合には署名を検証することによりデータを得、又は送られたデータが一時鍵 $K_{temp}$ で暗号化されている場合には署名を検証した後に一時鍵 $K_{temp}$ でデータを復号することによりデータを得る。この実施の形態において、相互認証後に送信されるデータについては、以上の方法により署名及び必要に応じて一時鍵 $K_{temp}$ による暗号化が施される場合がある。

ユーザ管理部 18 は、鍵サーバ 14 から配送鍵 $K_d$ を受信し、これを共有した一時鍵 $K_{temp}$ で暗号化して署名データを付加し、ユーザ登録データベースから登録情報を作成し、一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ 、署名データ、登録情報をユーザホームネットワーク 5 内の決済可能機器に送信する。登録情報の作成方法については、図 8 で説明した通りでありここでの詳細説明は省略する。

課金請求部 19 は、決済を実行するとき、経歴データ管理部 15 から課金情報、必要に応じて取扱方針、および価格情報を受信し、ユーザへの請求金額を算出し、請求情報を出納部 20 に送信する。出納部 20 は、銀行等と通信し、決済処理を実行する。その際、ユーザの未払い料金等の情報があれば、それらの情報は決済報告の形で課金請求部 19 およびユーザ管理部 18 に送信され、ユーザ登録データベースに反映され、以降のユーザ登録処理、または決済処理時に参照される。

一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ 、署名データ、登録情報を受信したユーザホームネットワーク 5 内の決済可能機器は、記憶してあった登録情報を更新すると共に、登録情報を検査し、登録がなされていれば、署名データを検証した



後、配送鍵 $K_d$ を一時鍵 $K_{temp}$ で復号化し、暗号処理部内の記憶モジュールに記憶されている配送鍵 $K_d$ を更新し、記憶モジュール内の課金情報を削除する。続いて、登録情報から代理決済すべき対象機器を検索し、当該検索により見つかった機器ごとに相互認証を行い、暗号処理部の記憶モジュールから読み出した配送鍵 $K_d$ を検索により見つかった機器ごとに異なる一時鍵 $K_{temp}$ で暗号化し、それぞれの機器ごとに署名を付け登録情報と共にそれぞれの機器に送信する。代理決済すべき対象機器が全て終わった時点で処理が終了する。

これらのデータを受信した対象機器は、決済可能機器と同様に登録情報を検査し、署名データを検証した後、配送鍵 $K_d$ を一時鍵 $K_{temp}$ で復号化し、記憶モジュール内の配送鍵 $K_d$ を更新し、課金情報を削除する。

なお、登録情報の登録項目が「登録不可」となっていた機器については、課金が行われなかったため、配送鍵 $K_d$ の更新、課金情報の削除は行わない（登録項目の内容は、使用を含めて一切の停止、購入処理の停止、処理が正常に行われた状態等、記述されていない種々の場合があり得る）。

図54は電子配信サービスセンタ1の利益分配処理の動作を説明する図である。経歴データ管理部15は、ユーザ管理部18から送信された課金情報、必要に応じて取扱方針、および価格情報を保持・管理する。利益分配部16は、経歴データ管理部15から送信された課金情報、必要に応じて取扱方針および価格情報からコンテンツプロバイダ2、サービスプロバイダ3、および電子配信サービスセンタ1それぞれの利益を算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、および出納部20に送信する。出納部20は、銀行等と通信し、決済を行う。サービスプロバイダ管理部11は、利益分配部16から受信した分配情報をサービスプロバイダ2に送信する。コンテンツプロバイダ管理部12は、利益分配部16から受信した分配情報をコンテンツプロバイダ3に送信する。

監査部21は、経歴データ管理部15から課金情報、取扱方針、および価格情報を受信し、データに矛盾がないか監査する。例えば、課金情報内の価格が価格

情報のデータと一致しているかどうか、分配率が一致しているかどうか等を監査し、取扱方針と価格情報が矛盾していないかどうか監査する。また、監査部 21 の処理としては、ユーザホームネットワーク 5 から入金された金額と、利益分配した合計金額又はサービスプロバイダ 3 へ送った金額との整合性を監査する処理や、ユーザホームネットワーク 5 の機器から供給された課金情報内のデータに例えば存在し得ないコンテンツプロバイダ ID、サービスプロバイダ ID や考えられない取り分、価格等が含まれているか否かを監査する処理がある。

図 5 5 は、電子配信サービスセンタ 1 の、コンテンツの利用実績を J A S R A C に送信する処理の動作を説明する図である。経歴データ管理部 1 5 は、ユーザのコンテンツの利用実績を示す課金情報を著作権管理部 1 3 および利益分配部 1 6 に送信する。利益分配部 1 6 は、課金情報から J A S R A C に対する請求金額および支払金額を算出し、支払情報を出納部 2 0 に送信する。出納部 2 0 は、銀行等と通信し、決済処理を実行する。著作権管理部 1 3 は、ユーザのコンテンツの利用実績を J A S R A C に送信する。

次に、EMD システムの処理について説明する。図 5 6 は、このシステムのコンテンツの配布および再生の処理を説明するフローチャートである。ステップ S 4 0 において、電子配信サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 は、コンテンツプロバイダ 2 に個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  およびコンテンツプロバイダ 2 の公開鍵証明書を送信し、コンテンツプロバイダ 2 がこれを受信する。その処理の詳細は、図 5 7 のフローチャートを参照して後述する。ステップ S 4 1 において、ユーザは、ユーザホームネットワーク 5 の機器（例えば、図 1 5 のホームサーバ 5 1）を操作し、ユーザホームネットワーク 5 の機器を電子配信サービスセンタ 1 のユーザ管理部 1 8 に登録する。この登録処理の詳細は、図 5 9 のフローチャートを参照して後述する。ステップ S 4 2 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、ユーザホームネットワーク 5 と、図 5 2 について上述したように相互認証した後、ユーザホームネットワーク 5 の機器に、配送鍵  $K_d$  を送信する。ユーザホームネットワーク 5 はこ

の鍵を受信する。この処理の詳細は、図 6 2 のフローチャートを参照して説明する。

ステップ S 4 3 において、コンテンツプロバイダ 2 の署名生成部 3 8 は、コンテンツプロバイダセキュアコンテナを生成し、それをサービスプロバイダ 3 に送信する。この処理の詳細は、図 6 5 のフローチャートを参照して後述する。ステップ S 4 4 において、サービスプロバイダ 3 の署名生成部 4 5 は、サービスプロバイダセキュアコンテナを生成し、それをユーザホームネットワーク 5 へ、ネットワーク 4 を介して送信する。この送信処理の詳細は、図 6 6 のフローチャートを参照して後述する。ステップ S 4 5 において、ユーザホームネットワーク 5 の購入モジュール 9 4 は、購入処理を実行する。購入処理の詳細は、図 6 7 のフローチャートを参照して後述する。ステップ S 4 6 において、ユーザは、ユーザホームネットワーク 5 の機器でコンテンツを再生する。再生処理の詳細は、図 7 2 のフローチャートを参照して後述する。

図 5 7 は、図 5 6 の S 4 0 に対応する、電子配信サービスセンタ 1 がコンテンツプロバイダ 2 へ個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  および公開鍵証明書を送信し、コンテンツプロバイダ 2 がこれを受信する処理の詳細を説明するフローチャートである。ステップ S 5 0 において、電子配信サービスセンタ 1 の相互認証部 1 7 は、コンテンツプロバイダ 2 の相互認証部 3 9 と相互認証する。この相互認証処理は、図 5 2 で説明したので、その詳細は省略する。相互認証処理により、コンテンツプロバイダ 2 が正当なプロバイダであることが確認されたとき、ステップ S 5 1 において、コンテンツプロバイダ 2 は、電子配信サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 から送信された個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  および証明書を受信する。ステップ S 5 2 において、コンテンツプロバイダ 2 は受信した個別鍵  $K_i$  を耐タンパメモリ 4 0 A に保存し、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$  および証明書をメモリ 4 0 B に保存する。

このように、コンテンツプロバイダ 2 は、電子配信サービスセンタ 1 から個別

鍵 $K_i$ 、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ および証明書を受け取る。同様に、図56に示すフローチャートの処理を行う例の場合、コンテンツプロバイダ2以外に、サービスプロバイダ3も、図57と同様の処理で、電子配信サービスセンタ1から個別鍵 $K_i$ （コンテンツプロバイダ2の個別鍵 $K_i$ とは異なる）、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ および証明書を受け取る。

なお、メモリ40Aは、コンテンツプロバイダ2が秘密裏に保持しなくてはならない個別鍵 $K_i$ を保持するため、第3者に容易にデータを読み出されない耐タンパメモリが望ましいが、特にハードウェア的制限は必要ない（例えば、入室管理された部屋の中にあるハードディスクや、パスワード管理されたパソコンのハードディスク等でよい）。また、メモリ40Bは、配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 、コンテンツプロバイダ2の証明書が保存されるだけであるため、通常の記憶装置等何でもよい（秘密にする必要がない）。また、メモリ40A、40Bを一つにしてもかまわない。

図58は、ホームサーバ51が、電子配信サービスセンタ1のユーザ管理部18に決済情報を登録する処理を説明するフローチャートである。ステップS60において、ホームサーバ51は、大容量記憶部68に記憶されている公開鍵証明書を、暗号処理部65の相互認証モジュール95で、電子配信サービスセンタ1の相互認証部17と相互認証する。この認証処理は、図52を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS60で、ホームサーバ51が電子配信サービスセンタ1のユーザ管理部18に送信する証明書は、図32に示すデータ（ユーザ機器の公開鍵証明書）を含む。

ステップS61において、ホームサーバは個人の決済情報（ユーザのクレジットカード番号や、決済機関の口座番号等）の登録が新規登録か否かを判定し、新規登録であると判定された場合、ステップS62に進む。ステップS62において、ユーザは入力手段63を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット112で一時鍵 $K_{temp}$ を用いて暗号化され、通信部61を介して電子配信サービスセンタ1のユーザ管理部18に送信される。

ステップS 6 3において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、受信した証明書から機器の I D を取り出し、この機器の I D を基に、図 7 に示したユーザ登録データベースを検索する。ステップS 6 4において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、受信した I D を有する機器の登録が可能であるか否かを判定し、受信した I D を有する機器の登録が可能であると判定された場合、ステップS 6 5 に進み、受信した I D を有する機器が、新規登録であるか否かを判定する。ステップS 6 5 において、受信した I D を有する機器が、新規登録であると判定された場合には、ステップS 6 6 に進む。

ステップS 6 6 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、決済 I D を新規に発行すると共に、一時鍵で暗号化された決済情報を復号化し、決済 I D および決済情報を、機器 I D、決済 I D、決済情報（口座番号やクレジットカード番号等）、取引停止情報等を記憶している決済情報データベースに機器の I D に対応させて登録し、決済 I D をユーザ登録データベースに登録する。ステップ 6 7 において、ユーザ登録データベースに登録したデータに基づき登録情報を作成する。この登録情報は、図 8 で説明しているので、その詳細は省略する。

ステップS 6 8 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、作成した登録情報をホームサーバ 5 1 に送信する。ステップS 6 9 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、受信した登録情報を大容量記憶部 6 8 に保存する。

ステップS 6 1 において、決済情報の登録が更新登録であると判定された場合、手続きは、ステップS 7 0 に進み、ユーザは入力手段 6 3 を用いて個人の決済情報を入力する。これらのデータは、暗号化ユニット 1 1 2 で一時鍵  $K_{temp}$  を用いて暗号化され、既に決済登録時に発行された登録情報と共に通信部 6 1 を介して電子配信サービスセンタ 1 のユーザ管理部 1 8 に送信される。

ステップS 6 4 において、受信した I D を有する機器の登録が不可能であると判定された場合、ステップS 7 1 に進み、電子配信サービスセンタ 1 のユーザ管理

部 18 は、登録拒絶の登録情報を作成し、ステップ S 68 に進む。

ステップ S 65 において、受信した ID を有する機器が、新規登録でないと判定された場合、手続きは、ステップ S 72 に進み、電子配信サービスセンタ 1 のユーザ管理部 18 は、一時鍵で暗号化された決済情報を復号化し、機器の ID に対応させて決済情報登録データベースに更新登録し、ステップ S 67 に進む。

このように、ホームサーバ 51 は、電子配信サービスセンタ 1 に登録される。

図 59 は、登録情報に機器の ID を新規登録する処理を説明するフローチャートである。ステップ S 80 における相互認証処理は、図 52 で説明した処理と同様なため、説明を省略する。ステップ S 81 において、図 58 のステップ S 63 と同じであるためその説明は省略する。ステップ S 82 は、図 58 のステップ S 64 と同じであるためその説明は省略する。ステップ S 83 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、ユーザ登録データベース内の機器 ID に対応する登録項目を「登録」に設定し、機器 ID を登録する。ステップ S 84 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、ユーザ登録データベースに基づき、図 8 に示すような登録情報を作成する。ステップ S 85 は、図 58 のステップ S 68 と同じであるためその説明は省略する。ステップ S 86 は、図 58 のステップ S 69 と同じであるためその説明は省略する。

ステップ S 82 において、受信した ID を有する機器の登録が不可であると判定された場合、ステップ S 87 に進み、電子配信サービスセンタ 1 のユーザ管理部 18 は、登録拒絶の登録情報を作成し、ステップ S 85 に進む。

このように、ホームサーバ 51 は、電子配信サービスセンタ 1 に登録される。

図 60 は、既に登録された機器を経由し、別の機器を追加登録する際の処理を説明するフローチャートである。ここでは、ホームサーバ 51 が既に登録されており、そこに据置機器 52 を登録する例で説明する。ステップ S 90 において、ホームサーバ 51 は、据置機器 52 と相互認証する。相互認証処理は、図 52 で説明した処理と同様なため、説明を省略する。ステップ S 91 において、ホームサーバ 51 は、電子配信サービスセンタ 1 と相互認証する。ステップ S 92 にお

いて、ホームサーバ51は、大容量記憶部68から読み出した登録情報、およびステップS90で据置機器52と相互認証した際に入手した据置機器52の証明書を電子配信サービスセンタ1に送信する。ステップS93は、図59のステップS81と同じであるためその説明は省略する。ステップS94は、図59のステップS82と同じであるためその説明は省略する。ステップS95は、図59のステップS83と同じであるためその説明は省略する。ステップS96において、電子配信サービスセンタ1のユーザ管理部18は、ホームサーバ51から受信した登録情報に加え、据置機器52の情報を追加した登録情報を新規に作成する。ステップS97は、図59のステップS85と同じであるためその説明は省略する。ステップS98は、図59のステップS86と同じであるためその説明は省略する。

そして、ステップS99Aにおいてホームサーバ51は受信した登録情報を据置機器52に送信し、ステップS99Bにおいて据置機器52は受信した登録情報を小容量記憶部75に保存する。

ステップS94において、受信したIDを有する機器の登録が不可であると判定された場合、ステップS99に進み、電子配信サービスセンタ1のユーザ管理部18は、据置機器52のみ登録拒絶とした登録情報（従って、ホームサーバ51は登録済みのまま）を作成し、ステップS97に進む（ステップS91でホームサーバ51が電子配信サービスセンタ1と相互認証に成功しているということは、ホームサーバ51が登録可であることを意味している）。

かくして、据置機器52は、図60に示した処理手順により電子配信サービスセンタ1に追加登録される。

ここで、登録済の機器が登録の更新（登録情報の更新）を行うタイミングについて説明する。図61は登録情報の更新を行うか否かを種々の条件に基づいて判断する処理手順を示し、ステップS600においてホームサーバ51は配送鍵K<sub>d</sub>、登録情報又は課金情報のすい上げから予め決められた一定期間が経過したか否かを時計（図示せず）及び判断部（図示せず）によって判断する。ここで肯定

結果が得られると、このことは配送鍵 $K_d$ 、登録情報又は課金情報のすい上げから一定の期間が経過していることを表しており、このときホームサーバ51はステップS607に移って登録情報の更新処理を実行する。この処理については図62において後述する。

これに対してステップS600において否定結果が得られると、このことは配送鍵 $K_d$ 、登録情報又は課金情報のすい上げから一定の期間が経過していないこと、すなわち期間の経過について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ51はステップS601に移る。

ステップS601においてホームサーバ51は、コンテンツの購入回数が規定の回数に達しているか否かを判断する。ここで肯定結果が得られると、ホームサーバ51はステップS607に移って登録情報更新処理を実行し、これに対してステップS601において否定結果が得られると、このことはコンテンツの購入回数について登録情報の更新条件を満たしていないことを表していることによりホームサーバ51は続くステップS602に移る。

ステップS602において、ホームサーバ51は、コンテンツの購入金額が規定の金額に達しているか否かを判断する。ここで肯定結果が得られると、ホームサーバ51はステップS607に移って登録情報更新処理を実行し、これに対してステップS602において否定結果が得られると、このことはコンテンツの購入金額について登録情報の更新条件を満たしていないことを表していることによりホームサーバ51は続くステップS603に移る。

ステップS603において、ホームサーバ51は、配送鍵 $K_d$ の有効期限が切れているか否かを判断する。配送鍵 $K_d$ の有効期限が切れているか否かを判断する方法としては、配信されたデータの配送鍵 $K_d$ のバージョンが記憶モジュール92に保存されている3つのバージョンの配送鍵 $K_d$ のいずれかのバージョンと一致するか否か又は、最近の配送鍵 $K_d$ のバージョンより古いかなどを調べる。この比較結果が一致していない場合又は最近の配送鍵 $K_d$ のバージョンより古い場合には、記憶モジュール92内の配送鍵 $K_d$ の有効期限が切れていることにな



り、ホームサーバ51はステップS603において肯定結果を得ることによりステップS607に移って登録情報の更新処理を実行する。これに対してステップS603において否定結果が得られると、このことは配送鍵K<sub>d</sub>の有効期限について登録情報の更新条件を満たしていないことを表しており、このときホームサーバ51は続くステップS604に移る。

ステップS604において、ホームサーバ51は、当該ホームサーバ51に他機器が新規接続されたか否か、又は接続されていた他機器が切り離されたか否かといったネットワーク構成の変更の有無を判断する。ここで肯定結果が得られると、このことはネットワーク構成に変更があったことを表しており、このときホームサーバ51はステップS607に移って登録情報の更新処理を実行する。これに対してステップS604において否定結果が得られると、このことはネットワーク構成について登録情報の更新条件を満たしていないことを表しており、ホームサーバ51は続くステップS605に移る。

ステップS605において、ホームサーバ51は、ユーザからの登録情報更新要求があったか否かを判断し、登録情報更新要求があった場合にはステップS607に移って登録情報の更新処理を実行し、登録情報更新要求がなかった場合にはステップS606に移る。

ステップS606において、ホームサーバ51は接続された他の機器について上述のステップS600～ステップS605における更新判断を行い、更新すべき判断結果が得られたときステップS607に移って登録情報の更新処理を行い、これに対して更新すべき判断結果が得られないとき上述のステップS600から同様の処理を繰り返す。これにより、ホームサーバ51は登録情報の更新処理を行うタイミングを得ることができる。なお、ホームサーバ51が他の機器の更新開始条件を調べるのではなく、他の機器が独自に調べて、自らホームサーバ51に要求を出すようにしてもよい。

図62は、登録済みの機器が登録を更新（登録情報の更新）し、決済処理を行い、配送鍵K<sub>d</sub>の再配布を受ける動作を説明するフローチャートである。ステッ

ステップS100における相互認証処理は、図52で説明した処理と同様なため、説明を省略する。ステップS101において、ホームサーバ51は、記憶モジュール92に記憶されている課金情報を、暗号処理部96の暗号化ユニット112で一時鍵 $K_{temp}$ を用いて暗号化し、署名生成ユニット114で署名を生成し、署名を付加する。そして、暗号化された課金情報及びその署名と、大容量記憶部68に記憶されている取扱方針、価格情報および登録情報を合わせて電子配信サービスセンタ1に送信する。なお、このとき、取扱方針および価格情報はモデルによっては送信する必要がない。なぜなら、コンテンツプロバイダ2およびサービスプロバイダ3が予め電子配信サービスセンタ1に送信している場合があったり、課金情報に取扱方針、価格情報のうちの必要な情報が含まれている場合があるからである。

ステップS102は、図59のステップS81と同じであるためその説明は省略する。ステップS103は、図59のステップS82と同じであるためその説明は省略する。ステップS104において、電子配信サービスセンタ1のユーザ管理部18は署名検証ユニット115で署名を検証し、受信した課金情報を一時鍵 $K_{temp}$ で復号化し（受信データに電子署名がついている場合には、署名検証ユニット115で検証する）、（受信していれば）取扱方針および価格情報と共に経歴データ管理部15に送信する。これを受信した経歴データ管理部15は、受信データを保存・管理する。

ステップS105において、電子配信サービスセンタ1のユーザ管理部18は、ユーザ登録データベース内の機器IDに対応する登録項目を検証すると共に、データを更新する。例えば、図示せぬ登録日付や課金状況などのデータである。ステップS106は、図59のステップS84と同じであるためその説明は省略する。ステップS107において、電子配信サービスセンタ1のユーザ管理部は、鍵サーバ14から供給された配送鍵 $K_d$ を一時鍵 $K_{temp}$ で暗号化し、登録情報と共にホームサーバ51に送信する。

ステップS108において、ホームサーバ51は受信した登録情報を大容量記

憶部 68 に保存する。ステップ S109 において、ホームサーバ 51 は、受信した登録情報を暗号処理部 65 に入力し、暗号処理部 65 では、登録情報に含まれる電子署名を署名検証ユニット 115 で検証すると共に、ホームサーバ 51 の機器 ID が登録されているか確認させ、検証に成功し、課金処理が完了したことを確認した際にはステップ S110 に進む。ステップ S110 において、ホームサーバ 51 は、受信した配送鍵  $K_d$  を暗号処理部 65 に入力する。暗号処理部 65 では、受信した配送鍵  $K_d$  を暗号/復号化モジュール 96 の復号化ユニット 111 で一時鍵  $K_{temp}$  を用いて復号化し、記憶モジュール 92 に保存（更新）し、記憶モジュール 92 に保持していた課金情報を消去する（これで、決済済みとなる）。

ステップ S103 において、受信した ID を有する機器の登録が不可であると判定された場合、ステップ S111 に進み、電子配信サービスセンタ 1 のユーザー管理部 18 は、登録拒絶とした登録情報を作成し、ステップ S112 に進む。ステップ S112 では、ステップ S107 と異なり、登録情報のみをホームサーバ 51 に送信する。

ステップ S109 において、登録情報に含まれる署名の検証に失敗するか、登録情報に含まれる「登録」の項目（例えば、課金処理失敗→購入処理ができない、登録拒否→再生等の処理を含め暗号処理部の機能の停止、取引一時停止→課金処理は成功したが、何らかの理由で購入を停止する、等が考えられる）に「登録可」が書かれていない場合は、ステップ S113 に進み所定のエラー処理を行う。

このように、ホームサーバ 51 は、登録情報を更新すると共に、課金情報を電子配信サービスセンタ 1 に送信し、代わりに配送鍵  $K_d$  の供給を受ける。

図 63 及び図 64 は、据置機器 52 がホームサーバ 51 を介して決済、登録情報の更新、配送鍵  $K_d$  の更新を行う処理を説明するフローチャートを示した図である。ステップ S120 において、ホームサーバ 51 の相互認証モジュール 94 と据置機器の図示せぬ相互認証モジュールは、相互認証を行う。相互認証処理は

、図 5 2 で説明した処理と同様なため、説明を省略する。なお、相互認証処理で説明したように、ホームサーバ 5 1 と据置機器 5 2 は互いに証明書を交換し合っているため、相手の機器 ID はわかっているものとする。ステップ S 1 2 1 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、大容量記憶部 6 8 から登録情報を読み出し、暗号処理部 6 5 に検査させる。上位コントローラ 6 2 から登録情報を受け取った暗号処理部 6 5 は、登録情報内の署名を検証し、据置機器の ID があるかどうか判定し、登録情報に据置機器の ID があつた際にはステップ S 1 2 2 に進む。

ステップ S 1 2 2 において、登録情報に据置機器 5 2 の ID が登録されているか否かを判定し、据置機器 5 2 の ID が登録されている場合には、ステップ S 1 2 3 に進む。ステップ S 1 2 3 において、据置機器 5 2 の暗号処理部 7 3 は、記憶モジュールに保存されている課金情報を読み出し、暗号化ユニットで一時鍵  $K_{temp}$  を用いて暗号化する。また、課金情報に対応する署名を、署名生成ユニットで生成する。署名の生成は図 1 0 で説明したのでその詳細は省略する。一時鍵  $K_{temp}$  で暗号化された課金情報およびその署名を受け取った上位コントローラ 7 2 は、必要に応じて課金情報に対応する取扱方針および価格情報を小容量記憶部 7 5 から読み出し、一時鍵  $K_{temp}$  で暗号化された課金情報とその署名、必要に応じて課金情報に対応する取扱方針および価格情報をホームサーバ 5 1 に送信する。

これらのデータを受信したホームサーバ 5 1 は、受信していれば取扱方針および価格情報を大容量記憶部 6 8 に記憶すると共に、一時鍵  $K_{temp}$  で暗号化された課金情報およびその署名を暗号処理部 6 5 に入力する。一時鍵  $K_{temp}$  で暗号化された課金情報およびその署名を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 で、一時鍵  $K_{temp}$  で暗号化された課金情報に対する署名を検証する。署名の検証は図 1 1 で説明した処理と同じであるため、その詳細は省略する。そして、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 は、一時鍵  $K_{temp}$  で暗号化された課金情報を復号化する。

ステップ S 1 2 4 において、ホームサーバ 5 1 は、電子配信サービスセンタ 1

の相互認証部 17 と相互認証し一時鍵  $K_{temp}$  2 を共有する。ステップ S 125 において、ホームサーバ 51 は、据置機器 52 から送られてきた課金情報を暗号／復号化モジュール 96 の暗号化ユニット 112 で一時鍵  $K_{temp}$  2 を用いて暗号化する。このとき、ホームサーバ 51 の課金情報を合わせて暗号化しておいてもよい。また、一時鍵  $K_{temp}$  2 で暗号化された課金情報に対応する署名を、暗号／復号化モジュール 96 の署名生成ユニット 114 で生成する。一時鍵  $K_{temp}$  2 で暗号化された課金情報、およびその署名を受け取った上位コントローラ 62 は、必要に応じて課金情報に対応する取扱方針、価格情報、および登録情報を大容量記憶部 68 から読み出し、一時鍵  $K_{temp}$  2 で暗号化された課金情報、その署名、必要に応じて課金情報に対応する取扱方針、価格情報および登録情報を電子配信サービスセンタ 1 のユーザ管理部 18 に送信する。

ステップ S 126 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、ユーザ登録データベースを検索する。ステップ S 127 において、ホームサーバ 51 および据置機器 52 がユーザ登録データベース内の「登録」の項目に、登録可で登録されているか否か判定し、登録されていると判定されていた場合、ステップ S 128 に進む。ステップ S 128 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、一時鍵  $K_{temp}$  2 で暗号化された課金情報に対する署名を検証し、課金情報を一時鍵  $K_{temp}$  2 で復号化する。そして、課金情報、受信していれば取扱方針および価格情報を経歴データ管理部 15 に送信する。課金情報、受信していれば取扱方針および価格情報を受信した経歴データ管理部 15 は、そのデータを管理・保存する。

ステップ S 129 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、ユーザ登録データベースを更新する（図示せぬ課金データ受信日時、登録情報発行日時、配送鍵交付日時等）。ステップ S 130 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、登録情報を作成する（例えば図 8 の例）。ステップ S 131 において、電子配信サービスセンタ 1 のユーザ管理部 18 は、電子配信サービスセンタ 1 の鍵サーバ 14 から受信した配送鍵  $K_d$  を一時鍵  $K_{temp}$  2

で暗号化し、一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ に対する署名を生成する。そして、登録情報、一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ に対する署名をホームサーバ51に送信する。

ステップS 1 3 2において、ホームサーバ51は、登録情報、一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ に対する署名を受信する。ホームサーバ51の上位コントローラ62は、一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ に対する署名を暗号処理部65に入力する。暗号処理部65において、暗号／復号化モジュール96の署名検証ユニット115は、一時鍵 $K_{temp}$  2で暗号化された配送鍵 $K_d$ に対する署名を検証し、暗号／復号化モジュール96の復号化ユニット111は、一時鍵 $K_{temp}$  2を用いて配送鍵 $K_d$ を復号化し、暗号／復号化モジュール96の暗号化ユニット112は、復号化された配送鍵 $K_d$ を、据置機器52との間で共有した一時鍵 $K_{temp}$ を用いて再暗号化する。最後に、暗号／復号化モジュール96の署名生成ユニット114は、一時鍵 $K_{temp}$ を用いて暗号化された配送鍵 $K_d$ に対応する署名を生成し、一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ に対する署名を上位コントローラ62に返送する。一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ に対する署名を受信した上位コントローラ62は、電子配信サービスセンタ1から送られてきた登録情報と共に据置機器52に送信する。

ステップS 1 3 3において、据置機器52の上位コントローラ72は、受信した登録情報を小容量記憶部75に上書き保存する。ステップS 1 3 4において、据置機器52の暗号処理部73は、受信した登録情報の署名を検証し、据置機器52のIDの「登録」に対する項目が「登録可」になっているか否かを判定し、「登録可」になっていた場合には、ステップS 1 3 5に進む。ステップS 1 3 5において、据置機器52の上位コントローラは、一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ および一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$ に対する署名を暗号処理部73に入力する。暗号処理部73は、一時鍵 $K_{temp}$ で暗号化された配送鍵 $K_d$

に対する署名を検証し、一時鍵  $K_{temp}$  を用いて配送鍵  $K_d$  を復号化し、暗号処理部 73 の記憶モジュール内の配送鍵  $K_d$  を更新すると共に、課金情報を消去する（なお、実際には消去せず、決済済みのマークを付けるだけの場合がある）。

ステップ S 1 2 1 において、据置機器 5 2 の ID が登録情報に含まれていなかった場合、ステップ S 1 3 6 に進み、図 6 0 で説明した登録情報追加処理を開始し、ステップ S 1 2 3 へと進む。

ステップ S 1 2 7 において、ユーザ登録データベース内の「登録」項目に対し、ホームサーバ 5 1 の ID または据置機器 5 2 の ID が「登録可」になっていなかった場合、ステップ S 1 3 7 に進む。ステップ S 1 3 7 は、ステップ S 1 3 0 の場合と同様なため、その詳細は省略する。ステップ S 1 3 8 は、ステップ S 1 3 1 において、電子配信サービスセンタ 1 のユーザ管理部 1 8 は、登録情報をホームサーバ 5 1 に送信する。ステップ S 1 3 9 において、ホームサーバ 5 1 は、登録情報を据置機器 5 2 に送信する。

ステップ S 1 2 2 において、登録情報における据置機器 5 2 の ID に対する「登録」項目が、「登録可」になっていなかった場合、ステップ S 1 3 4 において、登録情報における据置機器 5 2 の ID に対する「登録」項目が、「登録可」になっていなかった場合、処理は終了する。

なお、本方式による代理処理は、据置機器 5 2 のみの処理になっているが、ホームサーバ 5 1 につながる全ての機器やホームサーバ 5 1 自身の課金情報を全て集め、一括処理しても良い。そして、全ての機器の登録情報、配送鍵  $K_d$  の更新を行う（本実施例において、受け取った登録情報、配送鍵  $K_d$  は、ホームサーバ 5 1 で全くチェックされていない。ホームサーバ 5 1 自身の処理も一括して行う場合には、当然チェックし、更新すべきである）。

次に、図 5 6 のステップ S 4 3 に対応する、コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を、図 6 5 のフローチャートを用いて説明する。ステップ S 1 4 0 において、コンテンツプロバイダ 2 の電子透かし付加部 3 2 は、コンテンツサーバ 3 1 から読み出し

たコンテンツに、コンテンツプロバイダ2を示す所定のデータ、例えばコンテンツプロバイダIDなどを電子透かしの形で挿入し、圧縮部33に供給する。ステップS141において、コンテンツプロバイダ2の圧縮部33は、電子透かしが挿入されたコンテンツをATRAC等の所定の方式で圧縮し、コンテンツ暗号部34に供給する。ステップS142において、コンテンツ鍵生成部35は、コンテンツ鍵 $K_{\infty}$ として用いる鍵を生成させ、コンテンツ暗号部34およびコンテンツ鍵暗号部36に供給する。ステップS143において、コンテンツプロバイダ2のコンテンツ暗号部34は、DESなどの所定の方式で、コンテンツ鍵 $K_{\infty}$ を使用して、電子透かしが挿入され、圧縮されたコンテンツを暗号化する。

ステップS144において、コンテンツ鍵暗号部36は、DESなどの所定の方法で、図56のステップS40の処理により、電子配信サービスセンタ1から供給されている個別鍵 $K_i$ でコンテンツ鍵 $K_{\infty}$ を暗号化する。ステップS145において、取扱方針生成部37は、コンテンツの取り扱い方針を規定し、図33又は図34に示すような取扱方針を生成する。ステップS146において、コンテンツプロバイダ2の署名生成部38は、暗号化されたコンテンツ、暗号化されたコンテンツ鍵 $K_{\infty}$ 、暗号化された個別鍵 $K_i$ および取扱方針生成部37から供給された取扱方針に対し署名を生成する。署名の生成は図10を参照して説明した場合と同様であるので、ここでは説明を省略する。ステップS147において、コンテンツプロバイダ2は、暗号化されたコンテンツおよびその署名、暗号化されたコンテンツ鍵 $K_{\infty}$ およびその署名、暗号化された個別鍵 $K_i$ およびその署名、取扱方針およびその署名（以降、これら4つの署名付きデータをコンテンツプロバイダセキュアコンテナと呼ぶ）、予め認証局からもらっておいたコンテンツプロバイダ2の証明書を、図示せぬ送信部を用いてサービスプロバイダ3に送信する。

以上のように、コンテンツプロバイダ2は、サービスプロバイダ3に、コンテンツプロバイダセキュアコンテナを送信する。

次に、図56のステップS44に対応する、サービスプロバイダ3がホームサ



サーバ51にサービスプロバイダセキュアコンテナを送信する処理を、図66のフローチャートを用いて説明する。なお、サービスプロバイダ3は、コンテンツプロバイダ2から送信されたデータをコンテンツサーバ41に予め保存しているものとして説明する。ステップS150において、サービスプロバイダ3の証明書検証部42は、コンテンツサーバ41からコンテンツプロバイダ2の証明書の署名を読み出し、証明書内の署名を検証する。署名の検証は図11を参照して説明した方法と同様なため、その詳細は省略する。証明書に改竄がなければ、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ を取り出す。

ステップS151において、サービスプロバイダ3の署名検証部43は、コンテンツプロバイダ2の送信部から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵 $K_{pcp}$ で検証する（取扱方針の署名のみ検証する場合がある）。署名の検証に失敗し、改竄が発見された場合は、処理を終了する。なお、署名の検証は図11を参照して説明した方法と同様なため、その詳細は省略する。

コンテンツプロバイダセキュアコンテナに改竄がない場合、ステップS152において、サービスプロバイダ3の値付け部44は、取扱方針を基に、図37や図38で説明した価格情報を作成する。ステップS153において、サービスプロバイダ3の署名生成部45は、価格情報に対する署名を生成し、コンテンツプロバイダセキュアコンテナ、価格情報、および価格情報の署名を合わせサービスプロバイダセキュアコンテナを作成する。

ステップS154において、サービスプロバイダ3の図示せぬ送信部は、ホームサーバ51の通信部6.1に、サービスプロバイダ3の証明書、コンテンツプロバイダ2の証明書およびサービスプロバイダセキュアコンテナを送信し、処理を終了する。

このように、サービスプロバイダ3は、ホームサーバ51にサービスプロバイダセキュアコンテナを送信する。

図56のステップS45に対応する、適正なサービスプロバイダセキュアコン

テナを受信した後の、ホームサーバ51の購入処理の詳細を、図67のフローチャートを用いて説明する。ステップS161において、ホームサーバ51は図61及び図62について上述した登録情報更新処理を実行した後、ステップS162において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」の項目が「購入可」になっているか判定すると共に登録の項目が「登録可」になっていることを検査し、「購入可」及び「登録可」であった場合にはステップS163に進む。なお、署名検証、「登録可」、「購入可」の検査は登録情報検査モジュール93で行うようにしても良い。ステップS163において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。

コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップS164に進む。ステップS164において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツをホームサーバ51の暗号処理部65に入力する。コンテンツを受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツの署名を検証し、改竄がなされていないことが確認された場合には、ステップS165に進む。ステップS165において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツ鍵 $K_{co}$ をホームサーバ51の暗号処理部65に入力する。

コンテンツ鍵 $K_{co}$ を受信した暗号処理部65は、暗号／復号化モジュール96

の署名検証ユニット115でコンテンツ鍵 $K_c$ の署名を検証し、改竄がなされていないことが確認された場合には、ステップS166に進む。ステップS166において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した個別鍵 $K_i$ をホームサーバ51の暗号処理部65に入力する。個別鍵 $K_i$ を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115で個別鍵 $K_i$ の署名を検証し、改竄がなされていないことが確認された場合には、ステップS167に進む。

ステップS167において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した取扱方針をホームサーバ51の暗号処理部65に入力する。取扱方針を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115で取扱方針の署名を検証し、改竄がなされていないことが確認された場合には、ステップS168に進む。ステップS168において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したサービスプロバイダ3の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。

サービスプロバイダ3の公開鍵証明書を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115でサービスプロバイダ3の証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ3の公開鍵を取り出す。署名の検証の結果、改竄がなされていないことが確認された場合には、ステップS169に進む。ステップS169において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した価格情報をホームサーバ51の暗号処理部65に入力する。価格情報を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115で価格情報の署名を検証し、改竄がなされていないことが確認された場合には、ステップS170に進む。

ステップS170において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態

や価格など)を表示し、ユーザは入力手段63を用いて購入項目を選択する。入力手段63から入力された信号はホームサーバ51の上位コントローラ62に送信され、上位コントローラ62は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ51の暗号処理部65に入力する。なお、これらの入力処理は購入処理スタート時に行っても良い。これを受信した暗号処理部65は、ステップS167で入力された取扱方針およびステップS169で入力された価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図42で説明したので、その詳細は省略する。使用許諾条件情報については、図41で説明したので、その詳細は省略する。

ステップS171において、暗号処理部65の制御部91は、ステップS170で生成した課金情報を記憶モジュール92に保存する。ステップS172において、暗号処理部65の制御部91は、ステップS170で生成した使用許諾条件情報を暗号処理部65の外部メモリ制御部97に送信する。使用許諾条件情報を受信した外部メモリ制御部97は、外部メモリ67の改竄チェックを行った後、使用許諾条件情報を外部メモリ67に書き込む。書き込む際の改竄チェックについては、図69を用いて後述する。ステップS173において、暗号処理部65の制御部91は、ステップS166で入力された個別鍵 $K_i$ を、暗号/復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS165で入力されたコンテンツ鍵 $K_c$ を、暗号/復号化モジュール96の復号化ユニット111で、先ほど復号化した個別鍵 $K_i$ を用いて復号化する。最後に、暗号処理部65の制御部91は、暗号/復号化モジュール96の暗号化ユニット112で、記憶モジュール92から供給された保存鍵 $K_{save}$ を用いてコンテンツ鍵 $K_c$ を暗号化する。ステップS174において、保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ は、暗号処理部65の外部メモリ制御部97を経由して外部メモリ67に保存される。

ステップS162でホームサーバ51が購入処理できない機器であると判定さ

れた場合、又はステップS 1 6 3でコンテンツプロバイダ2の公開鍵証明書の署名が正しくないと判定された場合、又はステップS 1 6 4でコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップS 1 6 5で個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ の署名が正しくないと判定された場合、又はステップS 1 6 6で配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ の署名が正しくないと判定された場合、又はステップS 1 6 7で取扱方針の署名が正しくないと判定された場合、又はステップS 1 6 8でサービスプロバイダ3の証明書の署名が正しくないと判定された場合、又はステップS 1 6 9で価格情報の署名が正しくないと判定された場合、ホームサーバ5 1はステップS 1 7 6に進み、エラー処理を行う。なおステップS 1 6 5、およびステップS 1 6 6の処理をまとめ、コンテンツ鍵 $K_{co}$ 、個別鍵 $K_i$ に対する唯一の署名を検証するようにしてもよい。

以上のように、ホームサーバ5 1は、課金情報を記憶モジュール9 2に記憶すると共に、コンテンツ鍵 $K_{co}$ を個別鍵 $K_i$ で復号化した後、コンテンツ鍵 $K_{co}$ を保存鍵 $K_{save}$ で暗号化し、外部メモリ6 7に記憶させる。

据置機器5 2も、同様の処理で、課金情報を暗号処理部7 3の記憶モジュールに記憶すると共に、コンテンツ鍵 $K_{co}$ を個別鍵 $K_i$ で復号化し、コンテンツ鍵 $K_{co}$ を保存鍵 $K_{save}$  2（ホームサーバ5 1の鍵と異なる）で暗号化し、外部メモリ7 9に記憶させる。

図6 8は、暗号処理部6 5の外部メモリ制御部9 7が、外部メモリ6 7からデータを読み出す際に行う、改竄チェックの方法を説明するフローチャートである。図6 8のステップS 1 8 0において、暗号処理部6 5の外部メモリ制御部9 7は、外部メモリ6 7から読み出すデータの場所を検索する（例えば図1 6の1ブロック目の1番目のデータ）。ステップS 1 8 1において、暗号処理部6 5の外部メモリ制御部9 7は、外部メモリ6 7内の読み出し予定データを含む同一ブロック内全てのデータに対するハッシュ値（図1 6の1ブロック目全体のハッシュ値）を計算する。このとき、読み出し予定のデータ（例えばコンテンツ鍵1と使

用許諾条件情報 1) 以外は、ハッシュ値計算に使用後、破棄される。ステップ S 182 において、ステップ S 181 で計算したハッシュ値と暗号処理部 65 の記憶モジュール 92 に記憶されているハッシュ値 ( $ICV_1$ ) を比較する。一致していた場合、ステップ S 181 で読み出しておいたデータを、外部メモリ制御部 97 を介して制御部 91 に送信し、一致していなかった場合、外部メモリ制御部 97 はステップ S 183 に移り、当該メモリブロックは改竄されているものとして以降の読み書きを禁止する (不良ブロックとする)。例えば、外部メモリを 4 MB のフラッシュメモリとしたとき、このメモリを 64 のブロックに分けたものと仮定する。従って、記憶モジュールには 64 個のハッシュ値が記憶されている。データの読み出しを行う場合は、まず、データがある場所を検索し、そのデータを含む同一ブロック内の全てのデータに対するハッシュ値を計算する。このハッシュ値が、記憶モジュール内の当該ブロックに対応したハッシュ値と一致しているか否かで改竄をチェックする (図 16 参照)。

このように、暗号処理部 65 の外部メモリ制御部 97 は、外部メモリ 67 の改竄チェックを行い、データを読み出す。

図 69 は、暗号処理部 65 の外部メモリ制御部 97 が、外部メモリ 67 にデータを書き込む際に行う、改竄チェックの方法を説明するフローチャートである。図 69 のステップ S 190A において、暗号処理部 65 の外部メモリ制御部 97 は、外部メモリ 67 にデータを書き込むことができる場所を検索する。ステップ S 191A において、暗号処理部 65 の外部メモリ制御部 97 は、外部メモリ 67 内に空きエリアがあるか否か判定し、空きエリアがあると判定した場合、ステップ S 192A に進む。ステップ S 192A において、暗号処理部 65 の外部メモリ制御部 97 は、書き込み予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップ S 193A において、ステップ S 192A で計算したハッシュ値と暗号処理部 65 の記憶モジュール 92 に記憶されているハッシュ値を比較し、一致していた場合、ステップ S 194A に進む。ステップ S 194A において、書き込み予定領域にデータを書き込む。ステップ S 195A にお

いて、暗号処理部 6 5 の外部メモリ制御部 9 7 は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップ S 1 9 6 A において、制御部 9 1 は、暗号処理部 6 5 の記憶モジュール 9 2 内のハッシュ値をステップ S 1 9 5 A で計算したハッシュ値に更新する。

ステップ S 1 9 3 A において、計算したハッシュ値が記憶モジュール 9 2 内のハッシュ値と異なっていた場合、制御部 9 1 は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、ステップ S 1 9 0 A へ進む。

ステップ S 1 9 1 A において、外部メモリ 6 7 に空きエリアがないと判定された場合、ステップ S 1 9 8 A に進み、ステップ S 1 9 8 A において、外部メモリ制御部 9 7 は、書き込みエラーを制御部 9 1 に返送し、処理を終了する。

外部メモリ制御部 9 7 の外部メモリ 6 7 への書き換え（更新）方法は、図 7 0 に示すように、ステップ S 1 9 0 B において暗号処理部 6 5 の外部メモリ制御部 9 7 は、外部メモリ 6 7 のデータを書き換える場所を検索する。ステップ S 1 9 2 B において、暗号処理部 6 5 の外部メモリ制御部 9 7 は、書き換え予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップ S 1 9 3 B において、ステップ S 1 9 2 B で計算したハッシュ値と暗号処理部 6 5 の記憶モジュール 9 2 に記憶されているハッシュ値を比較し、一致していた場合、ステップ S 1 9 4 B に進む。ステップ S 1 9 4 B において、書き換え予定領域のデータを書き換える。ステップ S 1 9 5 B において、暗号処理部 6 5 の外部メモリ制御部 9 7 は、書き込んだデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップ S 1 9 6 B において、制御部 9 1 は、暗号処理部 6 5 の記憶モジュール 9 2 内のハッシュ値をステップ S 1 9 5 B で計算したハッシュ値に更新する。

ステップ S 1 9 3 B において、計算したハッシュ値が記憶モジュール 9 2 内のハッシュ値と異なっていた場合、制御部 9 1 は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、書き換え

失敗とする。

外部メモリ 79 のデータの削除方法について、図 7 1 を用いて説明する。ステップ S 190 C において、暗号処理部 73 の外部メモリ制御部は、外部メモリ 79 のデータを削除する場所を検索する。ステップ S 192 C において、暗号処理部 73 の外部メモリ制御部は、データ削除予定データブロック内の、全てのデータに対するハッシュ値を計算する。ステップ S 193 C において、ステップ S 192 C で計算したハッシュ値と暗号処理部 73 の記憶モジュール（図示せず）に記憶されているハッシュ値を比較し、一致していた場合、ステップ S 194 C に進む。ステップ S 194 C において、削除予定領域の削除予定であるデータを削除する。ステップ S 195 C において、暗号処理部 73 の外部メモリ制御部は、削除予定データを削除したデータブロック内の、全てのデータに対するハッシュ値を再計算する。ステップ S 196 C において、暗号処理部 73 は記憶モジュール内のハッシュ値をステップ S 195 C で計算したハッシュ値に更新する。

ステップ S 193 C において、計算したハッシュ値が記憶モジュール内のハッシュ値と異なっていた場合、暗号処理部 73 は、そのメモリブロックを不良ブロックとし（例えば、ハッシュ値を不良ブロックを示す値に変更する）、消去失敗とする。

図 5 6 のステップ S 46 に対応するホームサーバ 51 がコンテンツを再生する処理の詳細を、図 7 2 及び図 7 3 のフローチャートを用いて説明する。ステップ S 200 において、ホームサーバ 51 の上位コントローラ 62 は、ホームサーバ 51 の入力手段 63 から再生指示されたコンテンツに対応する ID を、ホームサーバ 51 の暗号処理部 65 に入力する。ステップ S 201 において、再生するコンテンツ ID を受信した暗号処理部 65 の制御部 91 は、コンテンツ ID を暗号処理部 65 の外部メモリ制御部 97 に送信し、コンテンツ ID に対応するコンテンツ鍵  $K_c$  および使用許諾条件情報を検索させる。このとき、使用許諾条件情報が再生可能な権利であることを確認する。ステップ S 202 において、暗号処理部 65 の外部メモリ制御部 97 は、コンテンツ鍵  $K_c$  および使用許諾条件情報を



含むデータブロックのハッシュ値を計算し、暗号処理部 65 の制御部 91 に送信する。ステップ S 203 において、暗号処理部 65 の制御部 91 は、暗号処理部 65 の記憶モジュール 92 に記憶されているハッシュ値とステップ S 202 で受信したハッシュ値が一致しているか否か判定し、一致していた場合にはステップ S 204 に進む。

ステップ S 204 において、暗号処理部 65 の制御部 91 は、使用許諾条件情報を必要に応じて更新する。例えば、使用許諾条件情報内の利用権が回数券であった場合、その回数を減算するなどの処理である。従って、更新する必要のない買い切りの権利などは、更新する必要がなく、その場合、ステップ S 208 へジャンプする（図示していない）。ステップ S 205 において、外部メモリ制御部 97 は、制御部 91 から送信された更新された使用許諾条件情報を、外部メモリ 67 に書き換え更新する。ステップ S 206 において、外部メモリ制御部 97 は、書き換えたデータブロック内の全データに対するハッシュ値を計算し直し、暗号処理部 65 の制御部 91 に送信する。ステップ S 207 において、暗号処理部 65 の制御部 91 は、暗号処理部 65 の記憶モジュール 92 に記憶されているハッシュ値を、ステップ S 206 で算出したハッシュ値に書き換える。

ステップ S 208 において、暗号処理部 65 と伸張部 66 は相互認証を行い、一時鍵  $K_{temp}$  を共有する。相互認証処理は、図 51 を用いて説明したのでその詳細は省略する。ステップ S 209 において、暗号／復号化モジュール 96 の復号化ユニット 111 は、外部メモリ 97 から読み出したコンテンツ鍵  $K_{co}$  を、記憶モジュール 92 から供給された保存鍵  $K_{save}$  で復号化する。ステップ S 210 において、暗号／復号化モジュール 96 の暗号化ユニット 112 は、先ほど伸張部 66 と共有した一時鍵  $K_{temp}$  でコンテンツ鍵  $K_{co}$  を再暗号化する。ステップ S 211 において、暗号処理部 65 の制御部 91 は、上位コントローラ 62 を介して、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$  を伸張部 66 に送信する。

ステップ S 212 において、伸張部 66 の鍵復号モジュール 102 は、相互認証モジュール 101 から供給された一時鍵  $K_{temp}$  でコンテンツ鍵  $K_{co}$  を復号化する。

る。ステップS 2 1 3において、上位コントローラ6 2は大容量記憶部6 8からコンテンツを読み出し、伸張部6 6に供給する。コンテンツを受信した伸張部6 6の復号モジュール1 0 3は、鍵復号モジュール1 0 2から供給されたコンテンツ鍵K<sub>0</sub>を用いてコンテンツを復号化する。ステップS 2 1 4において、伸張部6 6の伸張モジュール1 0 4は、コンテンツを所定の方式、例えばATRACなどの方式により伸張する。ステップS 2 1 5において、電子透かし付加モジュール1 0 5は、暗号処理部6 5から指示されたデータを電子透かしの形でコンテンツに挿入する（暗号処理部から伸張部へ渡されるデータは、コンテンツ鍵K<sub>0</sub>だけではなく、再生条件（アナログ出力、デジタル出力、コピー制御信号付き出力（SCMS））、コンテンツ利用権を購入した機器IDなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のID（つまりは、使用許諾条件情報内の機器ID）などである）。ステップS 2 1 6において、伸張部6 6は、図示せぬスピーカを介して音楽を再生する。

このように、ホームサーバ5 1は、コンテンツを再生する。

図7 4は、ホームサーバ5 1が据置機器5 2のために、コンテンツ利用権を代理購入する処理の詳細を説明したフローチャートである。ステップS 2 2 0において、ホームサーバ5 1と据置機器5 2は、相互認証する。相互認証処理は、図5 2で説明した処理と同様なため、説明を省略する。ステップS 2 2 1において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出した登録情報を、ホームサーバ5 1の暗号処理部6 5に検査させる。上位コントローラ6 2から登録情報を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5に、登録情報に付加されている署名を、暗号処理部6 5の記憶モジュール9 2から供給された電子配信サービスセンタ1の公開鍵で検証させる。署名の検証に成功した後、暗号処理部6 5の制御部9 1は、登録情報に据置機器のIDが登録され、「登録」及び「購入」の項目が「登録可」及び「購入化」になっているか判定し、「登録可」になっていると判定された場合にはステップS 2 2 2に進む（なお、据置機器5 2側でも登録

情報を検査し、ホームサーバ51が「登録可」になっていることを判定している)。ステップS225からステップS227は、図67のステップS160からステップS171までと同様な処理なため、その詳細は省略する。

ステップS228において、暗号処理部65の制御部91は、ステップS225で入力された配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を、暗号/復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS225で入力された個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号/復号化モジュール96の復号化ユニット111で、個別鍵 $K_i$ を用いて復号化する。そして、暗号処理部65の制御部91は、暗号/復号化モジュール96の暗号化ユニット112で、ステップS220の相互認証時に据置機器52と共有した一時鍵 $K_{temp}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。ステップS229において、暗号処理部65の制御部91は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS226で生成した使用許諾条件情報に対し、暗号/復号化モジュール96の署名生成ユニット114を用いて署名を生成し、上位コントローラ62に送信する。一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ51の上位コントローラ62は、大容量記憶部68からコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ(署名を含む。以下同じ)を読み出し、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを据置機器52に送信する。

ステップS230において、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信した据置機器52は、署名を検証した後コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを据置機器52の記録再生部76に出力する。コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信した据置機器52の記録再生部76は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを記録メディア80に保存する。

ステップS 2 3 1において、据置機器5 2の暗号処理部7 3は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュールの復号化ユニットで、ステップS 2 2 0の相互認証時にホームサーバ5 1と共有した一時鍵 $K_{temp}$ を用いて復号化する。そして、暗号処理部7 3の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部7 3の記憶モジュールから供給された保存鍵 $K_{save}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。

ステップS 2 3 2において、据置機器5 2の暗号処理部7 3は、保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ とステップS 2 3 0で受信した使用許諾条件情報を暗号処理部7 3の外部メモリ制御部に送信し、外部メモリ7 9に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図6 9で説明しているので、詳細は省略する。

このように、ホームサーバ5 1はコンテンツ利用権を購入し、課金情報はホームサーバ5 1側で保存し、利用権は据置機器5 2に引き渡される。

図7 5は、ホームサーバ5 1が、既に購入済みのコンテンツ利用権を、別の利用形態に変更して購入するための処理を示したフローチャートである。図7 5のステップS 2 4 0からステップS 2 4 5までは、図6 7で説明した処理と同様であるため、その説明は省略する。ステップS 2 4 6において、ホームサーバ5 1の暗号処理部6 5は、暗号処理部6 5の外部メモリ制御部9 7に、利用権変更するコンテンツの使用許諾条件情報を読み出させる。外部メモリ6 7からのデータの読み出しは、図6 8を参照して説明したので、その詳細は省略する。ステップS 2 4 6で正常に使用許諾条件情報が読み出せた場合には、ステップS 2 4 7へ進む。

ステップS 2 4 7において、ホームサーバ5 1の上位コントローラ6 2は、表示手段6 4を用いて利用権内容変更可能なコンテンツの情報（例えば、利用権内容変更可能な利用形態や価格など）を表示し、ユーザは入力手段6 3を用いて利用権内容更新条件を選択する。入力手段6 3から入力された信号はホームサーバ5 1の上位コントローラ6 2に送信され、上位コントローラ6 2は、その信号に

基づいて利用権内容変更コマンドを生成し、利用権内容変更コマンドをホームサーバ51の暗号処理部65に入力する。これを受信した暗号処理部65は、ステップS243で受信した取扱方針、ステップS245で受信した価格情報およびステップS247で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

ステップS248は、図67のステップS171と同様なため、その詳細な説明は省略する。ステップS249において、暗号処理部65の制御部91は、ステップS247で生成した使用許諾条件情報を、暗号処理部65の外部メモリ制御部97に出力する。外部メモリ制御部97は、受信した使用許諾条件情報を外部メモリ67に上書き更新する。外部メモリ制御部97の外部メモリ67への書き換え（更新）方法は、図70で説明したので、その詳細は省略する。

ステップS246において、外部メモリ67に、権利内容変更コマンドに付加されたコンテンツIDに対応する使用許諾条件情報が見つからなかった場合、または、使用許諾条件情報が記憶されている外部メモリの記憶ブロックに改竄が発見された場合（図68を参照して説明済み）、ステップS251へ進み、所定のエラー処理を行う。

このように、ホームサーバ51は、既に購入した権利（使用許諾権条件情報に記述されている）と、取扱方針および価格情報を用いて新たな権利を購入し、利用権内容を変更することができる。

図76及び図77は、取扱方針および価格情報のルール部分の具体例を示したものである。図76において、取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、この取扱方針には例えば5つのルールが記述されている。ルール1は、権利項目が利用権内容番号1であるから、図44より、その権利は再生権、時間・回数制限なしの権利であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は¥350であり、コンテンツプロバイダ2の取り分は、価格の30%である

。ルール2は、権利項目が利用権内容番号2であるから、図44より、その権利は再生権、時間制限有り、回数制限なしの権利であることがわかる。また、利用可能期間が1時間であることが、パラメータの項目からわかる。最低販売価格は¥100であり、コンテンツプロバイダ2の取り分は、価格の30%である。ルール3は、権利項目が利用権内容番号6であるから、図44より、その権利は複製権（コピー制御信号なし）、時間制限なし、回数制限ありの権利であることがわかる。また、利用可能回数が1回であることが、パラメータの項目からわかる。最低販売価格は¥30であり、コンテンツプロバイダ2の取り分は、価格の30%である。

ルール4は、権利項目が利用権内容番号13であるから、図44より、その権利は利用内容変更であることがわかる。変更可能なルール番号は、#2（再生権、時間制限有り、回数制限なし）から#1（再生権、時間・回数制限なし）であることがパラメータの項目からわかる。最低販売価格は¥200であり、コンテンツプロバイダ2の取り分は、価格の20%である。最低販売価格がルール1より低く提示してあるのは、既に購入している権利を下取りして再購入すると考えているからであり、コンテンツプロバイダ2の取り分がルール1より低く提示してあるのは、実際の作業をする電子配信サービスセンタ1の取り分を増やすためである（コンテンツプロバイダ2は、権利内容変更時には作業がないため）。

ルール5は、権利項目が利用権内容番号14であるから、図44より、その権利は再配布であることがわかる。再配布可能条件は、ルール番号#1（再生権、時間・回数制限なし）を持っている機器が、ルール番号#1（再生権、時間・回数制限なし）を購入して再配布することであることが、パラメータの項目からわかる。最低販売価格は¥250であり、コンテンツプロバイダ2の取り分は、価格の20%である。最低販売価格がルール1より低く提示してあるのは、既に購入している権利をもつ機器が、同一コンテンツにつき再購入すると考えているからであり、コンテンツプロバイダ2の取り分がルール1より低く提示してあるのは、実際の作業をする電子配信サービスセンタ1の取り分を増やすためである（

コンテンツプロバイダ 2 は、再配付時には作業がないため)。

図 77 において、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、この価格情報にも例えば 5 つのルールが記述されている。ルール 1 は、取扱方針のルール # 1 に対する価格情報で、利用権内容番号 # 1 を購入する際に、価格が ¥ 500 で、サービスプロバイダ 3 の取り分が 30% であることを示す。従って、ユーザが支払う ¥ 500 は、コンテンツプロバイダ 2 が ¥ 150、サービスプロバイダ 3 が ¥ 150、電子配信サービスセンタ 1 が ¥ 200 取ることになる。ルール 2 からルール 5 までも同様であるので、その詳細は省略する。

なお、ルール 4、5 において、サービスプロバイダ 2 の取り分がルール 1 に比べて少ないのは、サービスプロバイダ 2 の配信作業をユーザ機器が代行して行っており、代金の回収は電子配信サービスセンタ 1 が行っているためである。

また本例ではルール番号が # 1 から # 5 へと連番となっているが、必ずしもその必要はない。作成者はルール番号ごとに利用権内容番号とパラメータを設定しておき、そこから抽出したものを並べるため、一般には連番にならない。

図 78 は、図 75 で説明した権利内容変更を行う際の具体的な例を示したものである。取扱方針は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータ、最低販売価格、コンテンツプロバイダの利益率から構成され、価格情報は利用権ごとに整理番号として付けられたルール番号、パラメータ及び価格情報から構成され、使用許諾条件情報は利用権ごとに整理番号として付けられたルール番号、利用権内容を示す利用権内容番号、そのパラメータから構成されている。ホームサーバ 51 は、既にルール番号 # 2 の再生権、時間制限ありの権利を購入しており、権利内容を示す使用許諾条件情報には、ルール番号 # 2 が記述されており、利用可能時間は残り 30 分で、今まで積算して 2 時間分の購入を行っていることを示している。今、時間制限ありから時間制限なしに変更しようとした場合、取扱方針のルール 3、価格情報のルール 3 および使用許諾条件情報から ¥ 200 で再生権、時間・回数制限なしに変

更でき、使用許諾条件情報は、ルール番号#1、利用権内容番号の再生権、時間・回数制限なしに変わることがわかる（利用権内容番号#1の場合のパラメータに関しては、後述する。また、本例で言えば、直接再生権、時間・回数制限なしを買う場合に比べ、一度、時間制限ありの権利を買ってから権利内容変更したほうが安くなってしまっている。このため、積算利用時間を見て割り引くようにした方がよい）。

図79は、ホームサーバ51が据置機器52のために、コンテンツ利用権を購入し、その利用権を再配布する処理の詳細を説明したフローチャートである。ステップS260からステップ264は、図74のステップS220からステップS225と同様なため、その詳細な説明は省略する。ステップS265において、ホームサーバ51の暗号処理部65は、暗号処理部65の外部メモリ制御部97に、再配布しようとするコンテンツに対応する使用許諾条件情報および保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_c$ を、外部メモリ67から読み出させる。外部メモリ制御部97による外部メモリ67の読み出し方法については、図68で説明したので、その詳細は省略する。読み出しに成功した場合は、ステップS266に進む。

ステップS266において、ホームサーバ51の上位コントローラ62は、表示手段64を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段63を用いて再配付条件を選択する。なお、この選択処理は、予め再配付処理スタート時に行うようにしても良い。入力手段63から入力された信号はホームサーバ51の上位コントローラ62に送信され、上位コントローラ62は、その信号に基づいて再配布コマンドを生成し、再配布コマンドをホームサーバ51の暗号処理部65に入力する。これを受信した暗号処理部65は、ステップS264で受信した取扱方針、価格情報およびステップS265で読み出した使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

ステップS267は、図67のステップS171と同様なため、その詳細な説



明は省略する。ステップS 2 6 8において、暗号処理部6 5の制御部9 1は、ステップS 2 6 5で読み出した保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュール9 6の復号化ユニット1 1 1で、記憶モジュール9 2から供給された保存鍵 $K_{save}$ を用いて復号化する。そして、暗号処理部6 5の制御部9 1は、暗号／復号化モジュール9 6の暗号化ユニット1 1 2で、ステップS 2 6 0の相互認証時に据置機器5 2と共有した一時鍵 $K_{temp}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。最後に、暗号／復号化モジュール9 6の署名生成ユニット1 1 4は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS 2 6 6で生成した新しい使用許諾条件情報に対応した署名を生成し、暗号処理部6 5の制御部9 1に返送する。

ステップS 2 6 9からステップS 2 7 2の処理は、図7 4のステップS 2 2 9からステップS 2 3 2と同様なため、その詳細は省略する。

このように、ホームサーバ5 1は、自己の保持する利用権（使用許諾条件情報）と取扱方針、価格情報から新しい使用許諾条件情報を作り出し、自己の保持するコンテンツ鍵 $K_{co}$ 、コンテンツとともに据置機器5 2へ送信することで、コンテンツの再配布が行える。

図8 0は、ホームサーバ5 1が据置機器5 2のために、使用許諾条件情報、コンテンツ鍵 $K_{co}$ を送信し、据置機器5 2でコンテンツ利用権を購入する処理の詳細を説明したフローチャートである。ステップS 2 8 0において、据置機器5 2の暗号処理部7 3は、暗号処理部7 3の記憶モジュールに記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合にはステップS 2 8 1に進む（なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い）。

ステップS 2 8 1において、据置機器5 2の上位コントローラ7 2は、据置機器5 2の小容量記憶部7 5から読み出した登録情報を据置機器5 2の暗号処理部7 3に入力する。登録情報を受信した暗号処理部7 3は、図示せぬ暗号／復号化モジュールの署名検証ユニットで登録情報の署名を検証した後、据置機器5 2の

1 Dに対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップS 2 8 2に進む。

ステップS 2 8 2は、図7 4のステップS 2 2 0と同様なため、その詳細は省略する。ステップS 2 8 3は、図7 4のステップS 2 2 1と同様なため、その詳細は省略する（ホームサーバ5 1は据置機器5 2が登録されているか否かを判定し、据置機器5 2はホームサーバ5 1が登録されているか否かを判定する）。ステップS 2 8 4は、図7 9のステップS 2 6 5と同様なため、その詳細は省略する。ステップS 2 8 5は、図7 9のステップS 2 6 8と同様なため、その詳細は省略する。ステップS 2 8 6において、暗号処理部6 5の制御部9 1は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS 2 8 4で読み出した使用許諾条件情報に対し、暗号／復号化モジュール9 6の署名生成ユニット1 1 4を用いて署名を生成し、上位コントローラ6 2に送信する。一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ5 1の上位コントローラ6 2は、大容量記憶部6 8からコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、必要に応じて取扱方針とその署名、価格情報とその署名を読み出し、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツ、取扱方針とその署名および価格情報とその署名を据置機器5 2に送信する。

ステップS 2 8 7は、図7 4のステップS 2 3 0と同様なため、その詳細は省略する。ステップS 2 8 8は、図7 4のステップS 2 2 5と同様なため、その詳細は省略する。ステップS 2 8 9において、据置機器5 2の上位コントローラ7 2は、表示手段7 8を用いて再配布可能なコンテンツの情報（例えば、再配布可能なコンテンツの利用形態や価格など）を表示し、ユーザは入力手段7 7を用いて再配付条件を選択する。なお、この選択処理は予め再配付処理スタート時に行うようにしても良い。入力手段7 7から入力された信号は据置機器5 2の上位コントローラ7 2に送信され、上位コントローラ7 2は、その信号に基づいて再配布コマンドを生成し、再配布コマンドを据置機器5 2の暗号処理部7 3に入力す

る。これを受信した暗号処理部 73 は、ステップ S 286 で受信した取扱方針、価格情報および使用許諾条件情報から、課金情報および新しい使用許諾条件情報を生成する。

ステップ S 290 において、据置機器 52 の暗号処理部 73 は、ステップ S 289 で生成した課金情報を暗号処理部 73 の図示せぬ記憶モジュールに保存する。ステップ S 291 において、据置機器 52 の暗号処理部 73 は、ステップ S 286 で受信した一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$  を、暗号処理部 73 の図示せぬ復号化ユニットで、ステップ S 282 で共有した一時鍵  $K_{temp}$  を用いて復号化する。そして、据置機器 52 の暗号処理部 73 は、暗号処理部 73 の図示せぬ暗号化ユニットで、暗号処理部 73 の図示せぬ記憶モジュールから供給された保存鍵  $K_{save}$  2 を用いてコンテンツ鍵  $K_{co}$  を暗号化する。

ステップ S 292 において、据置機器 52 の暗号処理部 73 は、ステップ S 289 で生成した使用許諾条件情報およびステップ S 291 で生成した保存鍵  $K_{save}$  2 で暗号化されたコンテンツ鍵  $K_{co}$  を暗号処理部 73 の図示せぬ外部メモリ制御部に送信する。使用許諾条件情報および保存鍵  $K_{save}$  2 で暗号化されたコンテンツ鍵  $K_{co}$  を受信した外部メモリ制御部は、使用許諾条件情報および保存鍵  $K_{save}$  2 で暗号化されたコンテンツ鍵  $K_{co}$  を外部メモリ 79 に書き込む。書き込む際の改竄チェックについては、図 69 を用いて説明したので、その詳細は省略する。

このように、据置機器 52 は、ホームサーバ 51 の保持する利用権（使用許諾条件情報）、取扱方針、価格情報、コンテンツ鍵  $K_{co}$ 、コンテンツをホームサーバ 51 から受信し、据置機器 52 で新しい使用許諾条件情報を作り出すことにより、コンテンツの再配布を受けることができる。

図 81 は、管理移動権について説明した図である。管理移動とは、機器 1 から機器 2 へ再生権を移動できる動作のことで、機器 1 から機器 2 へ権利が移動することは通常の移動と同じであるが、機器 2 は受け取った再生権を再移動することができない点で通常の移動と異なる（通常の移動と同様に、再生権を移動した後の機器 1 は、再生権の再移動できない）。再生権を管理移動で受け取った機器 2

は、再生権を機器 1 に返還することができ、返還された後は、機器 1 は再度再生権の移動ができ、機器 2 は引き続きできない。これらを実現するため、使用許諾条件情報に管理移動権の購入者および現在の管理移動権の保持者を管理させている（ここでは、利用権内容番号 # 1 を持っている場合にのみ管理移動できることを想定しているが、利用権内容番号 # 2 においても拡張できる）。

図 8 1 において、取扱方針のルール 1 は、図 7 8 で説明しているの、その詳細は省略する。ルール 2 は、権利項目が利用権内容番号 1 6 であるから、図 4 4 より、その権利は管理移動権であることがわかる。また、パラメータの項目には、特に記述がないことがわかる。最低販売価格は ¥ 1 0 0 であり、コンテンツプロバイダ 2 の取り分は、価格の 5 0 % である。コンテンツプロバイダ 2 の取り分がルール 1 より高く提示してあるのは、サービスプロバイダ 3 は実際の作業を全く行わないため、その分をコンテンツプロバイダ 2 への取り分に回したためである。

図 8 1 において、価格情報のルール 1 は、図 7 8 で説明しているの、その詳細は省略する。ルール 2 は、取扱方針のルール # 2 に対する価格情報で、利用権内容番号 # 1 6 を購入する際に、価格が ¥ 1 0 0 で、サービスプロバイダ 3 の取り分が 0 % であることを示す。従って、ユーザが支払う ¥ 1 0 0 は、コンテンツプロバイダ 2 が ¥ 5 0、サービスプロバイダ 3 が ¥ 0、電子配信サービスセンタ 1 が ¥ 5 0 取ることになる。

図 8 1 において、ユーザはまずルール番号 # 1（再生権、時間・回数制限無し）を購入する。ただし、このとき管理移動権は持っていない（図 8 1 の（a）の状態）。次に、ユーザは管理移動権を購入する（これらの動作は一瞬なため、ユーザは一括して購入したように見える）。使用許諾条件のルール番号は、購入者を示す暗号処理部の ID（以下購入者とする）が ID 1（例えば、ホームサーバ 5 1 の ID）、再生権を保有する暗号処理部の ID（以下保持者とする）が ID 2 になる（図 8 1 の（b）の状態）。これを、管理移動を行って据置機器 5 2 に移した場合、ホームサーバ 5 1 の持つ使用許諾条件情報のルール部は、購入者は

I D 1 のままだが、保持者が I D 2 に変化する。また、管理移動により再生権を受信した据置機器 5 2 の持つ使用許諾条件情報のルール部は、購入者は I D 1、保持者は I D 2 となり、ホームサーバ 5 1 の使用許諾条件情報と一緒にになっている。

図 8 2 は、管理移動権の移動処理の詳細を説明するフローチャートである。図 8 2 において、ステップ S 3 0 0 は、図 7 4 のステップ S 2 2 0 と同様なため、その詳細は省略する。また、ステップ S 3 0 1 は図 7 4 のステップ S 2 2 1 と同様なため、その詳細は省略する。ステップ S 3 0 2 は図 7 5 のステップ S 2 4 6 と同様であため、その詳細は省略する。ステップ S 3 0 3 において、ホームサーバ 5 1 の暗号処理部 6 5 は、読み出した使用許諾条件情報内のルール部を検査し、使用権が再生権、時間・回数制限なし、管理移動権ありになっているか判定する。管理移動権があると判定された場合、ステップ S 3 0 4 に進む。

ステップ S 3 0 4 において、暗号処理部 6 5 の制御部 9 1 は、管理移動権の購入者および保持者が、共にホームサーバ 5 1 の I D になっているか判定する。管理移動権の購入者および保持者が、共にホームサーバ 5 1 の I D になっていると判定された場合には、ステップ S 3 0 5 に進む。ステップ S 3 0 5 において、暗号処理部 6 5 の制御部 9 1 は、使用許諾条件情報の管理移動権の保持者を据置機器 5 2 の I D に書き換える。ステップ S 3 0 6 において、暗号処理部 6 5 の制御部 9 1 は、ステップ S 3 0 5 で書き換えた使用許諾条件情報を暗号処理部 6 5 の外部メモリ制御部 9 7 に出力する。使用許諾条件情報を受信した暗号処理部 6 5 の外部メモリ制御部 9 7 は、外部メモリ 6 7 に使用許諾条件情報を上書き保存する。外部メモリ 6 7 のデータを書き換え保存する方法については、図 7 0 で説明したので、その詳細は省略する。ステップ S 3 0 7 からステップ S 3 1 1 までは、図 7 9 のステップ S 2 6 8 からステップ S 2 7 2 と同様なため、その詳細は省略する。

ステップ S 3 0 3 で使用許諾条件情報に管理移動権が含まれていなかった場合、ステップ S 3 0 4 で管理移動権の購入者または保持者がホームサーバ 5 1 でな

かった場合は、処理を中断する。

このように、ホームサーバ51から据置機器52にコンテンツを再生するための権利を移動することができる。

図83は、現在管理移動権を所持している据置機器52から、管理移動権の購入者であるホームサーバ51に、管理移動権を返還させる処理について説明したフローチャートである。図83において、ステップS320は、図74のステップS220と同様なため、その詳細は省略する。ステップS321は図74のステップS221と同様であため、その詳細は省略するが、ホームサーバ51と据置機器52双方で相手のIDが登録されているか検査しているものとする。登録されていると判定された場合、ステップS322に進む。ステップS322は、図75のステップS246と同様であるため、その詳細は省略するが、ホームサーバ51と据置機器52双方で同一のコンテンツIDのデータを読み出していることとする。外部メモリからデータが正しく読めた場合には、ステップS323に進む。ステップS323は、図82のステップS303と同様であるため、その詳細は省略するが、ホームサーバ51と据置機器52双方で管理移動権があるか判定していることとする。管理移動権があると判定された場合には、ステップS324に進む。

ステップS324において、ホームサーバ51の暗号処理部65は、管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっているか判定する。管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっていると判定された場合には、ステップS325に進む。同様に、据置機器52の暗号処理部73は、管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっているか判定する。管理移動権の購入者がホームサーバ51のIDになっていて、保持者が据置機器52のIDになっていると判定された場合には、ステップS325に進む。

ステップS325において、据置機器52の記録再生部76は、記録メディア

80からコンテンツを削除する（ただし、暗号化されたデータが残るだけなので、無理に削除する必要はない）。ステップS326において、据置機器52の暗号処理部73は、暗号処理部73の図示せぬ外部メモリ制御部に、外部メモリ79に保存されている保存鍵 $K_{save}$ 2で暗号化されたコンテンツ鍵 $K_c$ と使用許諾条件情報を削除させる。外部メモリ79の照りの削除方法は図71で説明したので、その詳細は省略する。

ステップS327において、暗号処理部65の制御部91は、使用許諾条件情報の管理移動権の保持者をホームサーバ51のIDに書き換えた使用許諾条件情報を生成する。ステップS328において、暗号処理部65の制御部91は、ステップS327で生成した使用許諾条件情報を、暗号処理部65の外部メモリ制御部97に出力する。使用許諾条件情報を受信した暗号処理部65の外部メモリ制御部97は、外部メモリ67に使用許諾条件情報を上書き保存する。外部メモリ67に書き換え保存する方法については、図70で説明したので、その詳細は省略する。

ステップS321でホームサーバ51または据置機器52において、登録情報が改竄されていたり、相手の機器のIDが登録されていなかった場合、ステップS322でホームサーバ51または据置機器52において、外部メモリ内に所定のコンテンツに対するコンテンツ鍵または使用許諾条件情報が見つからなかったり、それらを含むメモリブロックが改竄されていた場合は、ステップS329へ進みエラー処理を行う。

ステップS323でホームサーバ51または据置機器52において、使用許諾条件情報内に管理移動権がなかった場合、ステップS324でホームサーバ51または据置機器52において、購入者がホームサーバ51で、保持者が据置機器52でなかった場合は、処理を中断する。

このように、据置機器52からホームサーバ51にコンテンツを再生するための権利をもどすことができる。

なお、コンテンツおよびコンテンツ鍵 $K_c$ 等を1つしか記述していないが、必

要に応じて複数存在することとする。

また、本例ではコンテンツプロバイダ 2 とサービスプロバイダ 3 が別々に扱われていたが、一つにまとめてしまってもよい。更にまた、コンテンツプロバイダ 2 の方式を、そのままサービスプロバイダ 3 に転用しても良い。

## (2) 個別鍵の使用による暗号化处理

コンテンツプロバイダ 2 は、図 9 について上述したようにコンテンツを自ら作成したコンテンツ鍵で暗号化する。また、コンテンツプロバイダ 2 は、電子配信サービスセンタ 1 からコンテンツプロバイダ固有の個別鍵と、配送鍵で暗号化された個別鍵を受け取り、個別鍵によってコンテンツ鍵を暗号化する。かくしてコンテンツプロバイダ 2 は、コンテンツ鍵で暗号化されたコンテンツと、個別鍵で暗号化されたコンテンツ鍵と、配送鍵で暗号化された個別鍵とをサービスプロバイダ 3 を介してユーザホームネットワーク 5 に供給する。

ユーザホームネットワーク 5 では、電子配信サービスセンタ 1 から受け取った配送鍵を用いてコンテンツプロバイダ固有の個別鍵を復号化する。これにより、ユーザホームネットワーク 5 はコンテンツプロバイダ 2 からコンテンツプロバイダ固有の個別鍵で暗号化されて供給されるコンテンツ鍵を復号することができる。コンテンツ鍵を得たユーザホームネットワーク 5 は当該コンテンツ鍵によりコンテンツを復号することができる。

ここで、個別鍵はコンテンツサーバごとに固有であるのに対して、配送鍵は一種類のみである。従って、ユーザホームネットワーク 5 は一種類の配送鍵だけを持っていれば、各コンテンツプロバイダからの個別鍵を復号することができる。従って、ユーザホームネットワーク 5 は各コンテンツプロバイダ固有の個別鍵を持つ必要がなくなり、配送鍵を持つだけですべてのコンテンツプロバイダのコンテンツを購入することができる。

また、各コンテンツプロバイダは、配送鍵を持たないことにより、他のコンテンツプロバイダ固有の個別鍵（配送鍵で暗号化されている）を復号することができない。これによりコンテンツプロバイダ間でのコンテンツの盗用を防止し得る。



。ここで、以上の実施の形態の構成と、特許請求の範囲に記載の発明の各手段とを明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

すなわち、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図 8 4 のコンテンツ送信装置 2 0 0）が持つ個別鍵保存用メモリ（例えば、図 8 4 の耐タンパメモリ 2 0 1）、コンテンツ鍵  $K_{co}$  を個別鍵  $K_i$  で暗号化するための手段（例えば、図 8 4 のデータ暗号部 2 0 3）、コンテンツ鍵  $K_{co}$  の使用条件等を記述した取扱方針を生成するための手段（例えば、図 8 4 の取扱方針生成部 2 0 6）、各種データに対してデジタル署名を生成するための手段（例えば、図 8 4 の署名生成部 2 0 7）と、コンテンツを購入するユーザ（例えば、図 8 4 のコンテンツ受信装置 2 1 0）が持つ各種データに対して生成された署名データを検証する手段（例えば、図 8 4 の署名検証部 2 2 2）、コンテンツ鍵  $K_{co}$  の生成者を示す ID と取扱方針の生成者の ID とを比較するための手段（例えば、図 8 4 の比較器 2 2 6）、配送鍵を保存するための手段（例えば、図 8 4 の耐タンパメモリ 2 2 1）とを備える。

また、本発明の情報送信システムにおいては、コンテンツ等の情報を送信するコンテンツ供給者又はコンテンツ販売業者（例えば、図 8 5 のコンテンツ送信装置 2 0 0）が持つ個別鍵保存用メモリ（例えば、図 8 5 の耐タンパメモリ 2 0 1）、鍵証明書を保存するためのメモリ（例えば、図 8 5 のメモリ 2 0 2）、コンテンツ鍵  $K_{co}$  を個別鍵  $K_i$  で暗号化するための手段（例えば、図 8 5 のデータ暗号部 2 0 3）、コンテンツを購入するユーザ（例えば、図 8 5 のコンテンツ受信装置 2 1 0）が持つ各種データに対して生成された署名データを検証する手段（例えば、図 8 5 の署名検証部 2 2 2）、配送鍵を保存するための手段（例えば、図 8 5 の耐タンパメモリ 2 2 1）とを備える。

### (3) 遠隔再生処理

コンテンツの再生権利を保持していない機器（例えば据置機器 5 2）でコンテンツを保持している機器（例えばホームサーバ 5 1）から再生コマンドを受け取り、コンテンツを再生する遠隔再生処理について説明する。

図 8 6 は遠隔再生処理手順を示し、まず、ユーザの入力操作によって遠隔再生しようとするコンテンツのコンテンツ ID が上位コントローラ 6 2 に入力された後、ステップ S 4 0 1 において、ホームサーバ 5 1 と据置機器 5 2 は相互認証する。相互認証処理は、図 5 2 で説明した処理と同様であるため、説明を省略する。ステップ S 4 0 2 において、ホームサーバ 5 1 の上位コントローラ 6 2 は、ホームサーバ 5 1 の大容量記憶部 6 8 から読み出した登録情報を、ホームサーバ 5 1 の暗号処理部 6 5 に検査させる。上位コントローラ 6 2 から登録情報を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 に、登録情報に付加されている署名を、暗号処理部 6 5 の記憶モジュール 9 2 から供給された認証局 2 2 の公開鍵で検証させる。署名の検証に成功した後、「登録」の項目が「登録可」になっているか判定し、「登録可」になっていると判定された場合にはステップ S 4 0 3 に進む。なお、据置機器 5 2 側でも登録情報を検査し、ホームサーバ 5 1 が「登録可」になっていることを判定している。

ステップ S 4 0 3 において上位コントローラ 6 2 は遠隔再生しようとするコンテンツのコンテンツ ID を含む再生コマンドを生成し、続くステップ S 4 0 4 において、ホームサーバ 5 1 の暗号処理部 6 5 は、暗号処理部 6 5 の外部メモリ制御部 9 7 に、遠隔再生しようとするコンテンツに対応する使用許諾条件情報及び保存鍵  $K_{save}$  で暗号化されたコンテンツ鍵  $K_c$  を、外部メモリ 6 7 から読み出させる。外部メモリ制御部 9 7 による外部メモリ 6 7 からのデータ読み出し方法については、図 6 8 で説明した通りであり、その詳細は省略する。読み出しに成功した場合、ステップ S 4 0 5 に進む。

ステップ S 4 0 5 において、暗号／復号化モジュール 9 6 の復号化ユニット 1 1 1 は、外部メモリ 6 7 から読み出したコンテンツ鍵  $K_c$  を、記憶モジュール 9

2から供給された保存鍵 $K_{save}$ で復号化する。ステップS406において、暗号／復号化モジュール96の暗号化ユニット112は、一時鍵 $K_{temp}$ でコンテンツ鍵 $K_{co}$ を暗号化した後、ステップS407において再生コマンドを一時鍵 $K_{temp}$ で暗号化する。

ホームサーバ51は続くステップS408において、遠隔再生しようとするコンテンツ（コンテンツ鍵 $K_{co}$ で暗号化されている）を大容量記憶部68から読み出して、これを上述のステップS406及びS407において一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵及び再生コマンドと共に据置機器52に送信する。

ステップS409において、据置機器52はホームサーバ51から受け取ったコンテンツ鍵及び再生コマンドを一時鍵 $K_{temp}$ で復号化し、ステップS410において暗号処理部73と伸張部74は相互認証を行い、一時鍵 $K_{temp}$ 2を共有する。そしてステップS411において暗号処理部73は上述のステップS410において伸張部74と共有した一時鍵 $K_{temp}$ 2でコンテンツ鍵 $K_{co}$ 及び再生コマンドを暗号化する。ステップS412において、暗号処理部73は一時鍵 $K_{temp}$ 2で暗号化されたコンテンツ鍵 $K_{co}$ 及び再生コマンドを伸張部74に送信し、伸張部74はステップS413においてコンテンツ鍵 $K_{co}$ 及び再生コマンドを一時鍵 $K_{temp}$ 2で復号化する。

伸張部74はステップS414において、ホームサーバ51から上述のステップS408においてホームサーバ51から受け取ったコンテンツを上述のステップS413において復号化された再生コマンドに従って上述のステップS413において復号化されたコンテンツ鍵 $K_{co}$ で復号化する。そして伸張部74は当該復号化されたコンテンツをステップS415において所定の方式、例えばATRACなどの方式により伸張する。ステップS416において、上位コントローラ72は暗号処理部73から指示されたデータを電子透かしの形でコンテンツに挿入する。因みに、暗号処理部73から伸張部74へ渡されるデータは、コンテンツ鍵 $K_{co}$ 及び再生コマンドだけではなく、再生条件（アナログ出力、デジタル出力、コピー制御信号付き出力（SCMS））、コンテンツ利用権を購入した機器

IDなども含まれている。挿入するデータは、このコンテンツ利用権を購入した機器のID、つまりは、使用許諾条件情報内の機器IDなどである。ステップS417において、伸張部74は、図示せぬスピーカを介して音楽を再生する。

以上の構成において、ホームサーバ51はコンテンツと当該コンテンツの再生コマンド及びコンテンツ鍵 $K_c$ を据置機器52に送信することにより、コンテンツの再生権利を保持していない据置機器52は、再生コマンド及びコンテンツ鍵 $K_c$ を用いてコンテンツを再生することができる。従って、以上の構成によれば、コンテンツを保持する機器（コンテンツの再生権利を有する機器）に接続された複数の機器（据置機器等）において、コンテンツを再生することができる。

#### （４）予約購入処理

配送鍵の有効期限が切れる前にコンテンツの鍵変換を予め行っておき、コンテンツの購入予約を行うホームサーバの予約購入処理について説明する。図87に示す予約購入処理手順のステップS451において、ホームサーバ51は登録情報更新判断処理を行い、ステップS452に進む。登録情報更新判断処理については、図61及び図62で説明した通りであり、その詳細説明は省略する。但し、予約購入処理においては、図61のステップS601やS602で述べた購入個数や購入金額に基づく登録情報更新タイミングの判断は行わなくても良い。

ステップS452において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定し、「購入可」及び「登録可」であった場合にはステップS453に進む。ステップS453において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部

65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、上位コントローラ62はステップS454に進む。

ステップS454においてホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツ鍵 $K_{co}$ をホームサーバ51の暗号処理部65に入力する。コンテンツ鍵 $K_{co}$ を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115でコンテンツ鍵 $K_{co}$ の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS455に進む。

ステップS455において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した個別鍵 $K_i$ をホームサーバ51の暗号処理部65に入力する。個別鍵 $K_i$ を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115で個別鍵 $K_i$ の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS456に進む。

ここで、個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ 及び配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ 全体に対して1つの署名がついている場合は、S454及びS455を1つに合わせることができ署名検証処理を簡略化できる。

ステップS456において、暗号処理部65の制御部91は、ステップS455で入力された個別鍵 $K_i$ を、暗号／復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS454で入力されたコンテンツ鍵 $K_{co}$ を、暗号／復号化モジュール96の復号化ユニット111で、先ほど復号化した個別鍵 $K_i$ を用いて復号化する。最後に、暗号処理部65の制御部91は、暗号／復号化モジュール96の暗号化ユニット112で、記憶モジュール92から供給された保存鍵 $K_{sav}$ を用いてコンテンツ鍵 $K_{co}$ を暗号化する。

ステップS 4 5 7において、保存鍵 $K_{save}$ で暗号化されたコンテンツ鍵 $K_{co}$ は、暗号処理部6 5の外部メモリ制御部9 7を経由して外部メモリ6 7に保存される。

また、ステップS 4 5 2でホームサーバ5 1が購入処理できない機器であると判定された場合、又はステップS 4 5 3でコンテンツプロバイダ2の公開鍵証明書の署名が正しくないと判定された場合、又はステップS 4 5 4で個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ の署名が正しくないと判定された場合、又はステップS 4 5 5で配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ の署名が正しくないと判定された場合、ホームサーバ5 1はステップS 4 5 8に進み、エラー処理を行う。

以上のように、ホームサーバ5 1は、コンテンツ鍵 $K_{co}$ を個別鍵 $K_i$ で復号化した後、コンテンツ鍵 $K_{co}$ を保存鍵 $K_{save}$ で再暗号化し、外部メモリ6 7に記憶させる。この予約購入処理は、実際にコンテンツを購入しないので、図6 7について上述した購入処理のうち、ステップS 1 6 1の登録情報更新判断処理のなかの課金情報についての処理、ステップS 1 6 4に対応する購入コンテンツについての処理、ステップS 1 6 7に対応する取扱い方針についての処理、ステップS 1 6 8に対応するサービスプロバイダの公開鍵検証についての処理、ステップS 1 6 9に対応する価格情報の署名検証についての処理、ステップS 1 7 0乃至ステップS 1 7 2に対応する課金情報及び使用許諾条件情報の保存処理は行わなくても良い。

因みに、図8 7の予約購入処理の場合、ホームサーバ5 1は使用許諾条件情報の作成は行わなかったが、これに代えて使用許諾条件情報を作成しその利用権内容番号（すなわち権利項目）を初期値等の権利を持っていない状態（例えば、存在しない# 0など）としておくようにしても良い。

このようにして、予約購入処理では、ホームサーバ5 1は配送鍵 $K_d$ の有効期限が切れる前にコンテンツ鍵 $K_{co}$ を外部メモリ6 7に保存しておくことにより、当該保存されたコンテンツ鍵 $K_{co}$ によって暗号化されたコンテンツについて、配送鍵 $K_d$ の期限に関わらず購入することができる。

ここで、ホームサーバ51において外部メモリ6.7にコンテンツ鍵 $K_c$ を保存することにより購入の予約がなされたコンテンツの本購入処理について説明する。図88に示す本購入処理手順のステップS471において、ホームサーバ51は登録情報更新判断処理を行い、ステップS472に進む。登録情報更新判断処理については、図61及び図62で説明した通り、その詳細は、省略する。但し、本購入処理においては、図61のステップS603で述べた配送鍵 $K_d$ に基づく登録情報更新タイミングの判断は行わなくて良い。

ステップS472において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出した登録情報をホームサーバ51の暗号処理部65に入力する。登録情報を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115で登録情報の署名を検証した後、ホームサーバ51のIDに対する「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか判定し、「購入可」及び「登録可」であった場合にはステップS473に進む。ステップS473において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツプロバイダ2の公開鍵証明書をホームサーバ51の暗号処理部65に入力する。コンテンツプロバイダ2の公開鍵証明書を受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115でコンテンツプロバイダ2の公開鍵証明書の署名を検証した後、公開鍵証明書からコンテンツプロバイダ2の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップS474に進む。

ステップS474において、ホームサーバ51の上位コントローラ62は、ホームサーバ51の大容量記憶部68から読み出したコンテンツをホームサーバ51の暗号処理部65に入力する。コンテンツを受信した暗号処理部65は、暗号/復号化モジュール96の署名検証ユニット115でコンテンツの署名を検証し、改ざんがなされていないことが確認された場合には、ステップS475に進む。

ステップS 4 7 5において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出した取扱方針をホームサーバ5 1の暗号処理部6 5に入力する。取扱方針を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5で取扱方針の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS 4 7 6に進む。ステップS 4 7 6において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出したサービスプロバイダ3の公開鍵証明書をホームサーバ5 1の暗号処理部6 5に入力する。サービスプロバイダ3の公開鍵証明書を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5でサービスプロバイダ3の公開鍵証明書の署名を検証した後、公開鍵証明書からサービスプロバイダ3の公開鍵を取り出す。署名の検証の結果、改ざんがなされていないことが確認された場合には、ステップS 4 7 7に進む。

ステップS 4 7 7において、ホームサーバ5 1の上位コントローラ6 2は、ホームサーバ5 1の大容量記憶部6 8から読み出した価格情報をホームサーバ5 1の暗号処理部6 5に入力する。価格情報を受信した暗号処理部6 5は、暗号／復号化モジュール9 6の署名検証ユニット1 1 5で価格情報の署名を検証し、改ざんがなされていないことが確認された場合には、ステップS 4 7 8に進む。

ステップS 4 7 8において、ホームサーバ5 1の上位コントローラ6 2は、表示手段6 4を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段6 3を用いて購入項目を選択する。なお、購入項目の選択処理は本購入処理に先立って行うようにしても良い。入力手段6 3から入力された信号はホームサーバ5 1の上位コントローラ6 2に送信され、上位コントローラ6 2は、その信号に基づいて購入コマンドを生成し、購入コマンドをホームサーバ5 1の暗号処理部6 5に入力する。これを受信した暗号処理部6 5は、ステップS 4 7 5で入力された取扱方針及びステップS 4 7 7で入力された価格情報から課金情報及び使用許諾条件情報を生成する。課金情報に



については、図４２で説明した通りであり、その詳細は省略する。また、使用許諾条件情報については、図４１で説明した通りであり、その詳細は省略する。

ステップＳ４７９において、暗号処理部６５の制御部９１は、ステップＳ４７８で生成した課金情報を記憶モジュール９２に保存する。そしてステップＳ４８０において、暗号処理部６５の制御部９１は、ステップＳ４７８で生成した使用許諾条件情報を暗号処理部６５の外部メモリ制御部９７に送信する。使用許諾条件情報を受信した外部メモリ制御部９７は、外部メモリ６７の改ざんチェックを行った後、使用許諾条件情報を外部メモリ６７に書き込む。書き込む際の改ざんチェックについては、図６９について上述した通りであり、詳細説明は省略する（なお、権利なしの使用許諾条件情報がすでに書き込まれている場合には、図７０で説明した書き換え処理により使用許諾条件情報を書き換え更新する）。

因みに、ステップＳ４７２でホームサーバ５１が購入処理できない機器であったり、登録されていないと判定された場合、又はステップＳ４７３でコンテンツプロバイダ２の公開鍵証明書の署名が正しくないと判定された場合、又はステップＳ４７４でコンテンツ鍵 $K_c$ で暗号化されたコンテンツの署名が正しくないと判定された場合、又はステップＳ４７５で取扱方針の署名が正しくないと判定された場合、又はステップＳ４７６でサービスプロバイダ３の公開鍵証明書の署名が正しくないと判定された場合、又はステップＳ４７７で価格情報の署名が正しくないと判定された場合、ホームサーバ５１はステップＳ４８１に進み、エラー処理を行う。

以上のように、ホームサーバ５１ではユーザが購入選択したコンテンツについての課金情報を記憶モジュール９２に記憶すると共に、使用許諾条件情報を外部メモリ６７に記憶することにより、コンテンツの本購入処理を終了する。この本購入処理では、図８７について上述した予約購入処理で既に行われたコンテンツ鍵 $K_c$ の署名検証（ステップＳ４５４）及び個別鍵 $K_i$ の署名検証（ステップＳ４５５）、並びにコンテンツ鍵 $K_c$ のかけ替え処理（ステップＳ４５６）は行わない。

以上の構成において、ホームサーバ51では配送鍵 $K_d$ が更新される前に予約購入処理によりコンテンツ鍵 $K_c$ を外部メモリ67に保存しておくことにより、コンテンツ鍵 $K_c$ を復号化する際に必要となる配送鍵 $K_d$ が更新されても、コンテンツ鍵 $K_c$ は既に外部メモリ67に保存されているので、配送鍵 $K_d$ の有効期限が切れてもコンテンツを購入することができる。

#### (5) 代理購入処理

登録情報 (Registration List) が異なっている機器、すなわちグループが異なっている機器間においてコンテンツの授受を行う代理購入処理について説明する。この代理購入処理では、例えばホームサーバ51と当該ホームサーバ51に対してグループ外機器である携帯機器等との間でコンテンツを授受する場合について、ホームサーバ51側で課金する場合と、グループ外機器で課金を行う場合をそれぞれ説明する。この場合、図15について上述した据置機器52をグループ外機器として説明する。

図89はホームサーバ51がグループ外機器にコンテンツを渡し、ホームサーバ51が課金処理を行う場合の処理手順を示し、ステップS501において、ホームサーバ51とグループ外機器は、相互認証する。相互認証処理は、図52で説明した処理と同様であるため、説明を省略する。ステップS502において、ホームサーバ51とグループ外機器とは互いに登録情報を交換し、続くステップS503において互いに相手の登録情報を検査する。

すなわち、ホームサーバ51はグループ外機器から受け取った登録情報を、暗号処理部65に検査させる。グループ外機器からの登録情報を受信した暗号処理部65は、暗号／復号化モジュール96の署名検証ユニット115に、登録情報に付加されている署名を、暗号処理部65の記憶モジュール92から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部65の制御部91は、登録情報にグループ外機器のIDが登録され、「購入処理」及び「登録」の項目が「購入可」及び「登録可」になっているか否かを判定する。また、ホームサーバ51の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ5

1の登録情報にホームサーバ51のIDが登録され、「登録」の項目が「登録可」になっているか否かを判定する。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ51はステップS504に移る。

ステップS504からステップS510は、図67のステップS161からステップS171までと同様な処理なため、その詳細は省略する。

ステップS511において、暗号処理部65の制御部91は、ステップS508で入力された配送鍵 $K_d$ で暗号化された個別鍵 $K_i$ を、暗号/復号化モジュール96の復号化ユニット111で、記憶モジュール92から供給された配送鍵 $K_d$ を用いて復号化する。次に、暗号処理部65の制御部91は、ステップS508で入力された個別鍵 $K_i$ で暗号化されたコンテンツ鍵 $K_{co}$ を、暗号/復号化モジュール96の復号化ユニット111で、先ほど復号化した個別鍵 $K_i$ を用いて復号化する。そして、暗号処理部65の制御部91は、暗号/復号化モジュール96の暗号化ユニット112で、ステップS501の相互認証時にグループ外機器と共有した一時鍵 $K_{temp}$ を用いてコンテンツ鍵 $K_{co}$ を再暗号化する。ステップS512において、暗号処理部65の制御部91は、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ と、ステップS509で生成した使用許諾条件情報に対し、暗号/復号化モジュール96の署名生成ユニット114を用いて署名を生成し、上位コントローラ62に送信する。一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報およびそれらの署名を受信したホームサーバ51の上位コントローラ62は、大容量記憶部68からコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを読み出し、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツをグループ外機器に送信する。

ステップS513において、一時鍵 $K_{temp}$ で暗号化されたコンテンツ鍵 $K_{co}$ 、使用許諾条件情報、それらの署名およびコンテンツ鍵 $K_{co}$ で暗号化されたコンテンツを受信したグループ外機器は、コンテンツ鍵 $K_{co}$ で暗号化されたコンテンツをグループ外機器の記録再生部76に出力する。コンテンツ鍵 $K_{co}$ で暗号化され

たコンテンツを受信したグループ外機器の記録再生部 7 6 は、コンテンツ鍵  $K_{co}$  で暗号化されたコンテンツを記録メディア 8 0 に保存する。

ステップ S 5 1 4 において、グループ外機器の暗号処理部 7 3 は、上述のステップ S 5 1 2 でホームサーバから受け取った署名の検証を行うと共に、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_{co}$  を、暗号／復号化モジュールの復号化ユニットで、ステップ S 5 0 1 の相互認証時にホームサーバ 5 1 と共有した一時鍵  $K_{temp}$  を用いて復号化する。そして、暗号処理部 7 3 の制御部は、暗号／復号化モジュールの暗号化ユニットで、暗号処理部 7 3 の記憶モジュールから供給された保存鍵  $K_{save}$  2 を用いてコンテンツ鍵  $K_{co}$  を再暗号化する。

ステップ S 5 1 5 において、グループ外機器の暗号処理部 7 3 は、保存鍵  $K_{save}$  2 で暗号化されたコンテンツ鍵  $K_{co}$  とステップ S 5 1 3 で受信した使用許諾条件情報を暗号処理部 7 3 の外部メモリ制御部に送信し、外部メモリ 7 9 に保存させる。外部メモリ制御部が外部メモリにデータを書き込む処理については、図 6 9 で説明しているので、詳細は省略する。

このように、ホームサーバ 5 1 はコンテンツ利用権を購入し、課金情報はホームサーバ 5 1 側で保存し、利用権はグループ外機器に引き渡される。これにより、ホームサーバ 5 1 はグループ外機器に引き渡したコンテンツ利用権についてその支払いを行うことになる。

次に、図 9 0 はホームサーバ 5 1 がグループ外機器にコンテンツを渡し、グループ外機器が課金処理を行う場合の処理手順を示し、ステップ S 5 5 1 においてグループ外機器は、暗号処理部 7 3 (図 1 5) 内に記憶されている課金情報の課金の合計が、上限に達しているか否か判定し、上限に達していなかった場合にはステップ S 5 5 2 に進む (なお、課金合計上限で判定するのではなく、課金処理件数の上限で判定するようにしても良い)。

ステップ S 5 5 2 において、グループ外機器の上位コントローラ 7 2 は、外部メモリ 7 9 から読み出した登録情報を暗号処理部 7 3 に入力する。登録情報を受信した暗号処理部 7 3 は、その内部に設けられた暗号／復号化モジュールの署名

検証ユニットで登録情報の署名を検証した後、グループ外機器（据置機器 5 2）の ID に対する「購入処理」の項目が「購入可」になっているか判定し、「購入可」であった場合にはステップ S 5 5 3 に進む。

ステップ S 5 5 3 において、ホームサーバ 5 1 とグループ外機器は、相互認証する。相互認証処理は、図 5 2 で説明した処理と同様であるため、説明を省略する。ステップ S 5 5 4 において、ホームサーバ 5 1 とグループ外機器とは互いに登録情報を交換し、続くステップ S 5 5 5 において互いに相手の登録情報を検査する。

すなわち、ホームサーバ 5 1 はグループ外機器から受け取った登録情報を、暗号処理部 6 5 に検査させる。グループ外機器からの登録情報を受信した暗号処理部 6 5 は、暗号／復号化モジュール 9 6 の署名検証ユニット 1 1 5 に、登録情報に付加されている署名を、暗号処理部 6 5 の記憶モジュール 9 2 から供給された公開鍵で検証させる。署名の検証に成功した後、暗号処理部 6 5 の制御部 9 1 は、登録情報にグループ外機器の ID が登録され、「登録」の項目が「登録可」になっているか否かを判定する。また、ホームサーバ 5 1 の登録情報を受け取ったグループ外機器も、同様にしてホームサーバ 5 1 の登録情報にホームサーバ 5 1 の ID が登録され、「登録」の項目が「登録可」になっているか否かを判定する。なお、同様の処理をグループ外機器も行っている。そして、互いに相手の機器が登録されていることが確認されると、ホームサーバ 5 1 はステップ S 5 5 6 に移る。

ステップ S 5 5 6 において、ホームサーバ 5 1 の制御部 9 1 は、外部メモリ制御部 9 7 を介して外部メモリ 6 7 から既に購入済のコンテンツ鍵を読み出し、続くステップ S 5 5 7 においてコンテンツ鍵  $K_{co}$  を保存鍵  $K_{save}$  で復号化すると共に一時鍵  $K_{temp}$  で再暗号化し、それらの署名を生成する。

ステップ S 5 5 8 において、ホームサーバ 5 1 は、S 5 5 7 で生成した保存鍵  $K_{temp}$  で暗号化されたコンテンツ鍵と大容量記憶部 6 8 から読みだしたコンテンツ、取扱方針、価格情報をグループ外機器に送信する。ステップ S 5 5 9 におい

てグループ外機器は、ホームサーバ 5 1 から受け取ったコンテンツを記録メディア 8 0 に保存する。

ステップ S 5 6 0 において、グループ外機器（据置機器 5 2）は取扱方針、価格情報等の署名を検証した後、ステップ S 5 6 1 において、グループ外機器の上位コントローラ 7 2 は、表示手段 7 8 を用いて購入可能なコンテンツの情報（例えば、購入可能な利用形態や価格など）を表示し、ユーザは入力手段 7 7 を用いて購入項目を選択する。なお購入項目の選択処理は代理購入処理に先立って行うようにしても良い。入力手段 7 7 から入力された信号は上位コントローラ 7 2 に送信され、上位コントローラ 7 2 は、その信号に基づいて購入コマンドを生成し、購入コマンドを暗号処理部 7 3 に入力する。これを受信した暗号処理部 7 3 は、ステップ S 5 6 0 で入力された取扱方針および価格情報から課金情報および使用許諾条件情報を生成する。課金情報については、図 4 2 で説明したので、その詳細は省略する。使用許諾条件情報については、図 4 1 で説明したので、その詳細は省略する。

ステップ S 5 6 2 において、暗号処理部 7 3 は、ステップ S 5 6 1 で生成した課金情報を暗号処理部 7 3 内の記憶モジュールに保存する。ステップ S 5 6 3 において、暗号処理部 7 3 は、ステップ S 5 5 7 で暗号化されたコンテンツ鍵について、署名を検証すると共に一時鍵  $K_{temp}$  で復号化し、保存鍵  $K_{save}$  2 で再暗号化する。そしてステップ S 5 6 4 において、保存鍵  $K_{save}$  2 で暗号化されたコンテンツ鍵  $K_c$  は、暗号処理部 7 3 から外部メモリ 7 9 に保存される。

このように、ホームサーバ 5 1 は既に購入したコンテンツ利用権をグループ外機器に引き渡し、グループ外機器は課金情報も保存することにより、グループ外機器はグループ外のホームサーバ 5 1 から引き渡されたコンテンツ利用権についてその支払いを行うことになる。

以上の構成において、登録情報（Registration List）が異なっている機器間において、上述のステップ S 5 0 2 及びステップ S 5 5 4 について上述したように、互いの登録情報を交換することにより、登録された機器で

あることを確認した後一方の機器が有するコンテンツを他方の機器に引き渡すことができる。従って、以上の構成によれば、グループが異なる機器間においてコンテンツの授受を行うことができる。

なお、上述の実施の形態においては、購入処理の際にコンテンツの署名を検証したが、処理に時間がかかるため省略する場合がある。また、取扱方針又は価格情報に、検証の必要性の有無を記述し、それに従って動作する場合がある。

#### (6) 電子音楽配信システムの他の構成

図91は、他の構成の電子音楽配信システム400を説明する図である。かかる電子音楽配信システム400においては、パーソナルコンピュータ構成の電子配信サービスセンタ401に、コンテンツサーバ用及び信号処理用の2台のパーソナルコンピュータ402および403からなるコンテンツプロバイダ404と、同様にコンテンツサーバ用及び信号処理用の2台のパーソナルコンピュータ405および406からなるサービスプロバイダ407との信号処理用のパーソナルコンピュータ（以下、これを信号処理用パーソナルコンピュータと呼ぶ）403および406が接続されている。

また、サービスプロバイダ407の信号処理用パーソナルコンピュータ406には、コンテンツプロバイダ404の信号処理用パーソナルコンピュータ403が接続されると共に、ユーザホームネットワーク408に設けられたパーソナルコンピュータ構成のホームサーバ409がネットワーク4を介して接続されている。

そして、ユーザホームネットワーク408においては、ホームサーバ409に据置型の記録再生装置などの据置機器410と、携帯型の記録再生装置や携帯型の通信端末（携帯型情報機器や携帯電話機など）などの携帯機器411とが接続されて構成されている。

図92に示すように、電子配信サービスセンタ401においては、CPU（Central Processing Unit）などの制御部415にバス416を介してRAM（Random Access Memory）417、

ROM (Read Only Memory) 418、表示部419、入力部420、ハードディスクドライブ (HDD: Hard Disk Drive) 421 およびネットワークインターフェイス422が接続されて構成されている。

この場合、制御部415は、ROM418に予め格納された各種プログラムを読み出してRAM417上で展開することによりこれら各種プログラムに従って図2について上述した電子配信サービスセンタ1のサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、著作権管理部13、鍵サーバ14、経歴データ管理部15、利益配分部16、相互認証部17、ユーザ管理部18、課金請求部19、出納部20および監査部21と同様の処理を実行し得るようになされている。

また、制御部415は、システム全てに使用する鍵（配送鍵 $K_d$  および個別鍵 $K_i$  など）や、課金情報、価格情報、取扱方針、さらにはユーザ登録データベース等の各種情報をハードディスクドライブ421のハードディスクに記録することによりこれら各種情報を保持・管理している。

さらに、制御部415は、ネットワークインターフェイス422を介してコンテンツプロバイダ404、サービスプロバイダ407、ユーザホームネットワーク408およびJASRACなどと通信し得るようになされており、これにより、コンテンツプロバイダ404、サービスプロバイダ407、ユーザホームネットワーク408およびJASRACなどとの間で配送鍵 $K_d$ 、配送鍵 $K_d$ で暗号化した個別鍵 $K_i$ 、課金情報、価格情報、取扱方針、登録情報およびコンテンツの利用実績などの各種情報を授受し得るようになされている。

このようにしてパーソナルコンピュータ構成の電子配信サービスセンタ401は、各種プログラムに従って、図2について上述した電子配信サービスセンタ1と同様の機能を実現し得るようになされている。

因みに、電子配信サービスセンタ401においては、入力部420および表示部419を特には使用しないことによりこれら入力部420および表示部419を設けないようにしても良いが、ハードディスクドライブ421に記録している



各種情報などを確認するためなどに入力部 4 2 0 および表示部 4 1 9 を使用しても良い。

また、電子配信サービスセンタ 4 0 1 においては、ROM 4 1 8 に代えて各種プログラムをハードディスクドライブ 4 2 1 のハードディスクに予め記録しても良い。

図 9 3 は、コンテンツプロバイダ 4 0 4 の構成を示すブロック図であり、コンテンツサーバ用のパーソナルコンピュータ（以下、これをサーバ用パーソナルコンピュータと呼ぶ）4 0 2 は、CPU などの制御部 4 2 5 にバス 4 2 6 を介して RAM 4 2 7、ROM 4 2 8、表示部 4 2 9、入力部 4 3 0、ユーザに供給するコンテンツをハードディスクに記憶しているハードディスクドライブ 4 3 1 および IEEE (Institute of Electrical and Electronics Engineers) 1394 インターフェイス 4 3 2 が接続されて構成されている。

また、コンテンツプロバイダ 4 0 4 において、信号処理用パーソナルコンピュータ 4 0 3 は、CPU などの制御部 4 3 5 にバス 4 3 6 を介して RAM 4 3 7、ROM 4 3 8、表示部 4 3 9、入力部 4 4 0、ハードディスクドライブ 4 4 1、電子配信サービスセンタ 4 0 1 およびサービスプロバイダ 4 0 7 との接続用のネットワークインターフェイス 4 4 2、サーバ用パーソナルコンピュータ 4 0 2 の IEEE 1394 インターフェイス 4 3 2 と IEEE 1394 ケーブル 4 4 3 を介して接続される IEEE 1394 インターフェイス 4 4 4 が接続されて構成されている。

この場合、サーバ用パーソナルコンピュータ 4 0 2 の制御部 4 2 5 は、ROM 4 2 8 に予め格納された所定のプログラムを読み出して RAM 4 2 7 上で展開することにより当該プログラムに従って動作しており、信号処理用パーソナルコンピュータ 4 0 3 の制御部 4 3 5 から IEEE 1394 ケーブル 4 4 3 を介してコンテンツの読出命令が送信されると、その読出命令を IEEE 1394 インターフェイス 4 3 2 を介して取り込み、当該取り込んだコンテンツの読出命令に基づ

いてハードディスクドライブ 431 のハードディスクからコンテンツを読み出すと共に、その読み出したコンテンツを IEEE 1394 インターフェイス 432 から IEEE 1394 ケーブル 443 を介して信号処理用パーソナルコンピュータ 403 に送信する。

因みに、サーバ用パーソナルコンピュータ 402 においては、入力部 430 および表示部 429 を特には使用しないことによりこれら入力部 430 および表示部 429 を設けないようにしても良いが、ハードディスクドライブ 431 に記録しているコンテンツを確認したり、またはハードディスクドライブ 431 に新たにコンテンツを記憶したりコンテンツを削除する場合などに入力部 430 および表示部 429 を使用しても良い。

また、サーバ用パーソナルコンピュータ 402 においては、ROM 428 に代えてプログラムをハードディスクドライブ 431 のハードディスクに予め記録するようにしても良い。

一方、コンテンツプロバイダ 404 において、信号処理用パーソナルコンピュータ 403 の制御部 435 は、個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、コンテンツプロバイダ 404 の公開鍵証明書をハードディスクドライブ 439 のハードディスクに記録することによりこれら個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、コンテンツプロバイダ 404 の公開鍵証明書を保持・管理している。

そして、制御部 435 は、ROM 438 に予め格納された所定の各種プログラムを読み出して RAM 437 上で展開することによりこれら各種プログラムに従って、図 9 について上述したコンテンツプロバイダ 2 の電子透かし付加部 32、圧縮部 33、コンテンツ暗号部 34、コンテンツ鍵生成部 35、コンテンツ鍵暗号部 36、取扱方針生成部 37、署名生成部 38 および相互認証部 39 と同様の処理を実行し得るようになされている。

これにより、信号処理用パーソナルコンピュータ 403 は、配送鍵  $K_d$ 、配送鍵  $K_d$  で暗号化した個別鍵  $K_i$ 、取扱方針、コンテンツプロバイダセキュアコンテ

ナを電子配信サービスセンタ 401 およびサービスプロバイダ 407 との間でネットワークインターフェイス 442 を介して授受し得るようになされている。

このようにしてパーソナルコンピュータ構成のコンテンツプロバイダ 404 は、各種プログラムに従って、図 9 について上述したコンテンツプロバイダ 2 と同様の機能を実現し得るようになされている。

因みに、信号処理用パーソナルコンピュータ 403 においては、入力部 440 および表示部 439 を特には使用しないことによりこれら入力部 440 および表示部 439 を設けないようにしても良いが、ハードディスクドライブ 441 に記録している個別鍵  $K_i$ 、配送鍵  $K_d$  で暗号化された個別鍵  $K_i$ 、コンテンツプロバイダ 404 の公開鍵証明書などを確認するためなどに入力部 440 および表示部 439 を使用しても良い。

また、信号処理用パーソナルコンピュータ 403 においては、ROM 438 に代えて各種プログラムをハードディスクドライブ 441 のハードディスクに予め記録するようにしても良い。さらに、信号処理用パーソナルコンピュータ 403 においては、RAM 437 に耐タンパ性をもたせて個別鍵  $K_i$  を保持するようにしても良い。

さらに、コンテンツプロバイダ 404 においては、信号処理用パーソナルコンピュータ 403 と、サーバ用パーソナルコンピュータ 402 とを IEEE 1394 ケーブル 443 を介して接続するようにしたが、当該信号処理用パーソナルコンピュータ 403 と、サーバ用パーソナルコンピュータ 402 とを USB (Universal Serial Bus) ケーブルや RS-232C ケーブルなどの所定の信号ケーブルなどを介して有線接続したり、所定の無線通信手段を介して無線接続するようにしても良い。

図 94 は、サービスプロバイダ 407 の構成を示すブロック図であり、サーバ用パーソナルコンピュータ 405 は、CPU などの制御部 445 にバス 446 を介して RAM 447、ROM 448、表示部 449、入力部 450、コンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ 404 の公開鍵証明書

をハードディスクに記憶しているハードディスクドライブ４５１、IEEE 1394 インターフェイス４５２が接続されて構成されている。

また、サービスプロバイダ４０７において、信号処理用パーソナルコンピュータ４０６は、CPUなどの制御部４５４にバス４５５を介してRAM４５６、ROM４５７、表示部４５８、入力部４４９、ハードディスクドライブ４６０、電子配信サービスセンタ４０１およびコンテンツプロバイダ４０４との接続用のネットワークインターフェイス４６１、サーバ用パーソナルコンピュータ４０５のIEEE 1394 インターフェイス４５２とIEEE 1394 ケーブル４６２を介して接続されるIEEE 1394 インターフェイス４６３、ユーザホームネットワーク４０８とネットワーク４を介して接続するためのモデム４６４が接続されて構成されている。

この場合、サーバ用パーソナルコンピュータ４０５の制御部４４５は、ROM ４４８に予め格納された所定のプログラムを読み出してRAM ４４７上で展開することにより当該プログラムに従って動作しており、信号処理用パーソナルコンピュータ４０６の制御部４５４からIEEE 1394 ケーブル４６２を介してコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ４０４の公開鍵証明書と共にこれらの書込命令が与えられると、IEEE 1394 インターフェイス４５２を介して取り込み、当該取り込んだ書込命令に基づいてハードディスクドライブ４５１のハードディスクにコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ４０４の公開鍵証明書を書き込むと共に、信号処理用パーソナルコンピュータ４０６の制御部４５４からIEEE 1394 ケーブル４６２を介してコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ４０４の公開鍵証明書の読出命令が与えられると、その読出命令をIEEE 1394 インターフェイス４５２を介して取り込み、当該取り込んだ読出命令に基づいてハードディスクドライブ４５１のハードディスクからコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ４０４の公開鍵証明書を読み出すと共に、その読み出したコンテンツプロバイダセキュアコンテナおよびコン

コンテンツプロバイダ 404 の公開鍵証明書を IEEE 1394 インターフェイス 452 から IEEE 1394 ケーブル 462 を介して信号処理用パーソナルコンピュータ 406 に送信する。

因みに、サーバ用パーソナルコンピュータ 405 においては、入力部 450 および表示部 449 を特には使用しないことによりこれら入力部 450 および表示部 449 を設けないようにしても良いが、ハードディスクドライブ 451 に記録しているコンテンツプロバイダセキュアコンテナおよびコンテンツプロバイダ 404 の公開鍵証明書などを確認するなどのために入力部 450 および表示部 449 を使用しても良い。

また、サーバ用パーソナルコンピュータ 405 においては、ROM 448 に代えてプログラムをハードディスクドライブ 451 のハードディスクに予め記録するようにしても良い。

一方、サービスプロバイダ 407 において、信号処理用パーソナルコンピュータ 406 の制御部 454 は、サービスプロバイダ 407 の公開鍵証明書をハードディスクドライブ 460 のハードディスクに記録し、RAM 456 に耐タンパ性をもたせてサービスプロバイダ 407 の秘密鍵を保持・管理している。

そして、制御部 454 は、ROM 457 に予め格納された所定の各種プログラムを読み出して RAM 456 上で展開することによりこれら各種プログラムに従って、図 14 について上述したサービスプロバイダ 3 の証明書検証部 42、署名検証部 43、値付け部 44、署名生成部 45 および相互認証部 46 と同様の処理を実行し得るようになされている。

これにより、信号処理用パーソナルコンピュータ 406 は、価格情報、コンテンツプロバイダセキュアコンテナなどを電子配信サービスセンタ 401 およびコンテンツプロバイダ 407 との間でネットワークインターフェイス 442 を介して授受し得ると共に、サービスプロバイダセキュアコンテナをモデム 464 を介してユーザホームネットワーク 408 に送信し得るようになされている。

このようにしてパーソナルコンピュータ構成のサービスプロバイダ 407 は、

各種プログラムに従って、図 1 4 について上述したサービスプロバイダ 3 と同様の機能を実現し得るようになされている。

因みに、信号処理用パーソナルコンピュータ 4 0 6 においては、入力部 4 5 9 および表示部 4 5 8 を特には使用しないことによりこれら入力部 4 5 9 および表示部 4 5 8 を設けないようにしても良いが、ハードディスクドライブ 4 6 0 に記録しているサービスプロバイダ 4 0 7 の公開鍵証明書などを確認するためなどに入力部 4 5 9 および表示部 4 5 8 を使用しても良い。

また、信号処理用パーソナルコンピュータ 4 0 6 においては、ROM 4 5 7 に代えて各種プログラムをハードディスクドライブ 4 6 0 のハードディスクに予め記録するようにしても良い。

さらに、サービスプロバイダ 4 0 7 においては、信号処理用パーソナルコンピュータ 4 0 6 と、サーバ用パーソナルコンピュータ 4 0 5 とを IEEE 1 3 9 4 ケーブル 4 6 2 を介して接続するようにしたが、当該信号処理用パーソナルコンピュータ 4 0 6 と、サーバ用パーソナルコンピュータ 4 0 5 とを USB ケーブルや RS - 2 3 2 C ケーブルなどの所定の信号ケーブルなどを介して有線接続したり、所定の無線通信手段を介して無線接続するようにしても良い。

図 9 5 は、ユーザホームネットワーク 4 0 8 の構成を示すブロック図であり、パーソナルコンピュータ構成のホームサーバ 4 0 9 は、CPU などの制御部 4 6 5 にバス 4 6 6 を介して RAM 4 6 7、ROM 4 6 8、表示部 4 6 9、入力部 4 7 0、ハードディスクドライブ 4 7 1、IEEE 1 3 9 4 インターフェイス 4 7 2、サービスプロバイダ 4 0 7 とネットワーク 4 を介して接続するためのモデム 4 7 3、電子配信サービスセンタ 4 0 1 との接続用のネットワークインターフェイス 4 7 4 が接続されて構成されている。

また、ユーザホームネットワーク 4 0 8 において、据置機器 4 1 0 は、CPU などの制御部 4 7 5 にバス 4 7 6 を介して RAM 4 7 7、ROM 4 7 8、表示部 4 7 9、入力部 4 8 0、記録再生部 4 8 1、記録メディア 4 8 2 用のメディアインターフェイス 4 8 3、ホームサーバの IEEE 1 3 9 4 インターフェイス 4 7

2とIEEE1394ケーブル484を介して接続されるIEEE1394インターフェイス485が接続されて構成されている。

さらに、ユーザホームネットワーク408において、携帯機器411は、CPUなどの制御部490にバス491を介してRAM492、ROM493、表示部494、入力部495、ホームサーバのIEEE1394インターフェイス472とIEEE1394ケーブル496を介して接続されるIEEE1394インターフェイス497が接続されて構成されている。

この場合、ホームサーバ409の制御部465は、ROM468に予め格納された各種プログラムを読み出してRAM467上で展開することによりこれら各種プログラムに従って図15について上述したホームサーバ51の上位コントローラ62、暗号処理部65および伸張部66と同様の処理を実行し得るようになっている。

また、ホームサーバ409の表示部469は、図15について上述したホームサーバ51の表示手段64と同様の機能を有し、当該ホームサーバ409の入力部470は、図15について上述したホームサーバ51の入力手段63と同様の機能を有している。さらに、ホームサーバ409のハードディスクドライブ471は、図15について上述したホームサーバ51の大容量記憶部68と同様の機能を有すると共に、モデム473およびネットワークインターフェイス474並びにIEEE1394インターフェイス472は、図15について上述したホームサーバ51の通信部61と同様の機能を有し、当該ホームサーバ409のRAM467は、図15について上述したホームサーバ51の外部メモリ67と同様の機能を有している。

従って、パーソナルコンピュータ構成のホームサーバ409は、各種プログラムに従って、図15について上述したホームサーバ51と同様の機能を実現し得るようになされている。

因みに、ホームサーバ409においては、ROM468に代えて各種プログラムをハードディスクドライブ471のハードディスクに予め記録したり、当該ハ

ードディスクドライブ471を図15について上述した外部メモリ67と同様に機能させても良い。また、ホームサーバ409においては、サービスプロバイダ407および電子配信サービスセンタ401との通信形態によってはモデム473およびネットワークインターフェイス474を1つのモデムなどのインターフェイスとしても良い。さらに、ホームサーバ409においては、据置機器410および携帯機器411をUSBケーブルやRS-232Cケーブルなどの所定の信号ケーブルなどを介して有線接続したり、所定の無線通信手段を介して無線接続するようにしても良い。

一方、ユーザホームネットワーク408において、据置機器410の制御部475は、ROM478に予め格納された各種プログラムを読み出してRAM477上で展開することによりこれら各種プログラムに従って図15について上述した据置機器52の上位コントローラ72、暗号処理部73および伸張部74と同様の処理を実行し得るようになされている。

また、据置機器410の表示部479は、図15について上述した据置機器52の表示手段78と同様の機能を有すると共に、入力部480は、図15について上述した据置機器52の入力手段77と同様の機能を有し、IEEE1394インターフェイス485は、図15について上述した据置機器52の通信部71と同様の機能を有している。さらに、据置機器410の記録再生部481は、図15について上述した据置機器52の記録再生部76と同様の機能を有すると共に、記録メディア482は、図15について上述した据置機器52の記録メディア80と同様の機能を有し、当該据置機器410のRAM477は、図15について上述した据置機器52の外部メモリ79および小容量記憶部75と同様の機能を有している。

従って、ユーザホームネットワーク408の据置機器410は、各種プログラムに従って、図15について上述したユーザホームネットワーク5の据置機器52と同様の機能を実現し得るようになされている。

因みに、据置機器410においては、ハードディスクドライブを新たに設け、



ROM 478に代えて各種プログラムをそのハードディスクドライブのハードディスクに予め記録したり、当該ハードディスクドライブを図15について上述した据置機器52の外部メモリ79および小容量記憶部75と同様に機能させても良い。また、据置機器410においては、記録メディア482が半導体メモリ構成である場合には、所定のプログラムに従って制御部475に記録再生部481の機能を実現させても良い。

ユーザホームネットワーク408において、携帯機器411の制御部490は、ROM493に予め格納された各種プログラムを読み出してRAM492上で展開することによりこれら各種プログラムに従って図15について上述した携帯機器53の上位コントローラ82、暗号処理部83および伸張部84と同様の処理を実行し得るようになされている。

また、携帯機器411のRAM492は、図15について上述した携帯機器53の外部メモリ85と同様の機能を有し、IEEE1394インターフェイス497は、図15について上述した携帯機器53の通信部81と同様の機能を有している。さらに、この携帯機器411では、表示部494および入力部495をコンテンツの再生時に利用し得るようになされている。

従って、ユーザホームネットワーク408の携帯機器411は、各種プログラムに従って、図15について上述したユーザホームネットワーク5の携帯機器53と同様の機能を実現し得るようになされている。

因みに、携帯機器411においては、コンテンツの記録再生用に着脱自在な記録メディアを設けるようにしても良い。

以上の構成において、かかる電子音楽配信システム400においては、電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407およびユーザホームネットワーク408のホームサーバ409をそれぞれパーソナルコンピュータ構成とした。

従って、電子音楽配信システム400では、コンテンツの配信用として、電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ

407およびホームサーバ409をハード構成で新たに製作する必要がなく、既存のパーソナルコンピュータに各種プログラムをインストールするだけで、これらパーソナルコンピュータを用いてシステムを容易に構築することができる。

以上の構成によれば、パーソナルコンピュータ構成の電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407およびホームサーバ409を用いて電子音楽配信システム400を構築するようにしたことにより、既存のパーソナルコンピュータを容易に電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407およびホームサーバ409とすることができ、かくして、システム構築を容易、かつ簡易にし得る。

なお、かかる電子音楽配信システム400では、電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407、ホームサーバ409、据置機器410および携帯機器411をROM418、428、438、448、457、468、478、493に予め格納された各種プログラムに従って動作させるようにした場合について述べたが、各種プログラムが記録されたプログラム格納媒体を電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407、ホームサーバ409、据置機器410および携帯機器411にインストールすることにより、当該電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407、ホームサーバ409、据置機器410および携帯機器411をプログラム格納媒体に格納している各種プログラムや、当該プログラム格納媒体からハードディスクなどに移行させた各種プログラムに従ってそれぞれ動作させるようにしても良い。

因みに、電子配信サービスセンタ401、コンテンツプロバイダ404、サービスプロバイダ407、ホームサーバ409、据置機器410および携帯機器411を動作させるために用いるプログラム格納媒体としては、CD-ROM (Compact Disc-Read Only Memory) などのパッケージメディアのみならず、プログラムが一時的もしくは永続的に格納される半導体メモリや磁気ディスクなどで実現しても良い。また、これらプログラム格納媒

体にプログラムを格納する手段としては、ローカルエリアネットワークやインターネット、デジタル衛星放送などの有線および無線通信媒体を利用しても良く、ルータやモデムなどの各種通信インターフェイスを介在させて格納するようにしても良い。

#### 産業上の利用の可能性

本発明は、音楽、映像、ゲームプログラムなどのコンテンツを提供するプロバイダなどの情報送信装置や、当該提供されたコンテンツを受信するパーソナルコンピュータや携帯電話機などの情報受信装置、さらには、これら情報送信装置及び情報受信装置から構築されるネットワークシステムに利用することができる。

## 請 求 の 範 囲

1. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を生成する送信側制御手段と、

上記暗号化されたデータ及び上記取扱方針データと共に上記暗号化されたデータ及び上記取扱方針データに対する署名を上記データ受信装置に送信する送信手段とを具え、

上記データ受信装置は、

上記暗号化されたデータ及び上記取扱方針データに対する署名を上記暗号化されたデータ及び上記取扱方針データと共に受信する受信手段と、

受信した上記署名の検証を行うと共に、上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する受信側制御手段とを具える

ことを特徴とする情報送信システム。

2. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成する送信側制御手段と、

上記データ用署名及び取扱方針用署名を上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する送信手段とを具え、

上記データ受信装置は、

上記データ用署名及び取扱方針用署名を上記暗号化されたデータ及び上記取扱方針データと共に受信する受信手段と、

上記データ用署名及び上記取扱方針用署名の検証を行うと共に、上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する受信側比較手段とを具える

ことを特徴とする情報送信システム。

3. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を生成する送信側制御手段と、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する送信手段とを具え、

上記データ受信装置は、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を上記暗号化されたデータ及び上記取扱方針データと共に受信する受信手段と、

上記セキュアコンテナ用署名の検証を行う受信側制御手段とを具える

ことを特徴とする情報送信システム。

4. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名の生成を行う送信側制御手段と、

上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信する送信手段とを具え、

上記データ受信装置は、

上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を受信する受信手段と、

上記データ用署名及び上記取扱方針用署名の検証を行う受信側制御手段とを具える

ことを特徴とする情報送信システム。

5. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信システムにおいて、

上記データ送信装置は、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記取扱方針データに対する取扱方針用署名を生成し、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成する送信側制御手段と、

上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信する送信手段とを具え、

上記データ受信装置は、

上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を受信する受信手段と、

上記データ用署名及び上記取扱方針用署名の検証を行う検証手段とを具えることを特徴とする情報送信システム。

6. 上記送信側制御手段は、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化鍵データに対する鍵データ用署名を生成し、

上記送信手段は、

上記生成された鍵データ用署名を上記データ受信装置に送信し、

上記受信手段は、

上記鍵データを受信し、

上記受信側制御手段は、

上記鍵データ用署名の検証を行う

ことを特徴とする請求の範囲第1項、第2項、第4項又は第5項に記載の情報送信システム。

7. 上記送信側制御手段は、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化されたデータ、上記暗号化鍵データ及び上記取扱方針に対するセキュアコンテナ用署名の生成を行い、

上記送信手段は、

上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記セキュアコンテナ用署名を上記データ受信装置に送信し、

上記受信手段は、

上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記セキュアコンテナ用署名を受信し、

上記受信側制御手段は、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第3項に記載の情報送信システム。

8. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信方法において、

上記データ送信装置により、上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を生成して上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する送信ステップと、

上記データ受信装置により、上記暗号化されたデータ及び上記取扱方針データに対する署名を上記暗号化されたデータ及び上記取扱方針データと共に受信し、上記署名の検証を行うと共に、上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する比較ステップとを具えることを特徴とする情報送信方法。

9. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信方法において、

上記データ送信装置により、上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成して、当該生成されたデータ用署名及び取扱方針用署名を上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する送信ステップと、

上記データ受信装置により、上記データ用署名及び取扱方針用署名を上記暗号化されたデータ及び上記取扱方針データと共に受信し、上記データ用署名及び上記取扱方針用署名の検証を行うと共に、上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する比較ステップとを具えることを特徴とする情報送信方法。

10. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信方



法において、

上記データ送信装置により、上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を生成して上記暗号化されたデータ及び上記取扱方針データと共に上記データ受信装置に送信する送信ステップと、

上記データ受信装置により、上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を上記暗号化されたデータ及び上記取扱方針データと共に受信し、上記セキュアコンテナ用署名の検証を行う検証ステップとを具えることを特徴とする情報送信方法。

1 1. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信方法において、

上記データ送信装置により、上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名の生成を行い、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信する送信ステップと、

上記データ受信装置により、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を受信し、上記データ用署名及び上記取扱方針用署名の検証を行う検証ステップと

を具えることを特徴とする情報送信方法。

1 2. データ送信装置とデータ受信装置とを用いてデータを送信する情報送信方法において、

上記データ送信装置により、上記データを所定の鍵データで暗号化すると共に

、上記データの取り扱い方針を記述した取扱方針データを生成し、上記取扱方針データに対する取扱方針用署名を生成し、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成して上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を上記データ受信装置に送信する送信ステップと、

上記データ受信装置により、上記暗号化されたデータ、上記データ用署名、上記取扱方針データ及び上記取扱方針用署名を受信し、上記データ用署名及び上記取扱方針用署名の検証を行う検証ステップと

を具えることを特徴とする情報送信方法。

1 3. 上記送信ステップは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化鍵データに対する鍵データ用署名を生成し、当該生成した鍵データ用署名を上記データ受信装置に送信し、

上記検証ステップは、

上記鍵データ用署名の検証を行う

ことを特徴とする請求の範囲第 8 項、第 9 項、第 1 1 項又は第 1 2 項に記載の情報送信方法。

1 4. 上記送信ステップは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化されたデータ、上記暗号化鍵データ及び上記取扱方針に対するセキュアコンテナ用署名の生成を行い、上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記セキュアコンテナ用署名を上記データ受信装置に送信し、

上記検証ステップは、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第 10 項に記載の情報送信方法。

15. 所定のデータをデータ受信装置に送信する情報送信装置において、  
上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針  
を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針  
データの送信用の署名を生成する送信側制御手段と、

上記暗号化されたデータ及び上記取扱方針データと共に上記署名を上記データ  
受信装置に送信する送信手段と

を具えることを特徴とする情報送信装置。

16. 上記送信側制御手段は、

作成者識別データを含む上記データを上記鍵データで暗号化すると共に、上記  
作成者識別データを含む上記取扱方針データを生成する

ことを特徴とする請求の範囲第 15 項に記載の情報送信装置。

17. 上記送信側制御手段は、

上記暗号化されたデータ及び上記取扱方針データに対する署名を生成する

ことを特徴とする請求の範囲第 15 項に記載の情報送信装置。

18. 上記送信側制御手段は、

上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成す  
る

ことを特徴とする請求の範囲第 15 項に記載の情報送信装置。

19. 上記送信側制御手段は、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用  
署名を生成する

ことを特徴とする請求の範囲第 15 項に記載の情報送信装置。

20. 上記送信側制御手段は、

上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名を生成する

ことを特徴とする請求の範囲第 15 項に記載の情報送信装置。

21. 上記送信側制御手段は、

上記取扱方針データに対する取扱方針用署名を生成し、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成する

ことを特徴とする請求の範囲第 15 項に記載の情報送信装置。

22. 上記送信側制御手段は、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化鍵データに対する鍵データ用署名を生成し、

上記送信手段は、

上記生成された鍵データ用署名を上記データ受信装置に送信する

ことを特徴とする請求の範囲第 15 項、第 16 項、第 17 項、第 18 項、第 20 項又は第 21 項に記載の情報送信装置。

23. 上記送信側制御手段は、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化されたデータ、上記暗号化鍵データ及び上記取扱方針に対するセキュアコンテナ用署名の生成を行い、

上記送信手段は、

上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記セキュアコンテナ用署名を上記データ受信装置に送信する

ことを特徴とする請求の範囲第 19 項に記載の情報送信装置。

24. データ送信装置から送信された所定のデータを受信する情報受信装置において、

上記データ送信装置から送信された、所定の鍵データで暗号化された上記データと、当該データの取り扱い方針を記述した取扱方針データと、上記暗号化されたデータ及び上記取扱方針データの送信用の署名とを受信する受信手段と、

受信した上記署名の検証を行う受信側制御手段と  
を具えることを特徴とする情報受信装置。

25. 上記受信側制御手段は、

上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する

ことを特徴とする請求の範囲第 24 項に記載の情報受信装置。

26. 上記受信手段は、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データに対する署名を受信し、

上記受信側制御手段は、

上記暗号化されたデータ及び上記取扱方針データに対する署名の検証を行う  
ことを特徴とする請求の範囲第 24 項に記載の情報受信装置。

27. 上記受信手段は、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データ毎の署名を受信し、

上記受信側制御手段は、

上記暗号化されたデータ及び上記取扱方針データ毎の署名の検証を行う

ことを特徴とする請求の範囲第 2 4 項に記載の情報受信装置。

28. 上記受信手段は、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を受信し、

上記受信側制御手段は、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第 2 4 項に記載の情報受信装置。

29. 上記受信手段は、

上記データ送信装置から送信された、上記暗号化されたデータに対するデータ用署名と、上記取扱方針データ及び上記データ用署名に対する取扱方針用署名とを受信し、

上記受信側制御手段は、

上記データ用署名と、上記取扱方針用署名との検証を行う

ことを特徴とする請求の範囲第 2 4 項に記載の情報受信装置。

30. 上記受信手段は、

上記データ送信装置から送信された、上記取扱方針データに対する取扱方針用署名と、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名とを受信し、

上記受信側制御手段は、

上記取扱方針用署名と、上記データ用署名との検証を行う

ことを特徴とする請求の範囲第 2 4 項に記載の情報受信装置。

31. 上記受信手段は、

上記データ送信装置から送信された、配送鍵で暗号化された上記鍵データに対

する鍵データ用署名を受信し、

上記受信側制御手段は、

上記鍵データ用署名の検証を行う

ことを特徴とする請求の範囲第 24 項、第 25 項、第 26 項、第 27 項、第 29 項又は第 30 項に記載の情報受信装置。

32. 上記受信手段は、

上記データ送信装置から送信された、配送鍵で暗号化された上記鍵データ、上記暗号化されたデータ及び上記取扱方針に対するセキュアコンテナ用署名を受信し、

上記受信側制御手段は、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第 28 項に記載の情報受信装置。

33. 所定のデータをデータ受信装置に送信する情報送信方法において、

上記データを所定の鍵データで暗号化すると共に、上記データの取り扱い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データの送信用の署名を生成する生成ステップと、

上記暗号化されたデータ及び上記取扱方針データと共に上記署名を上記データ受信方法に送信する送信ステップと

を具えることを特徴とする情報送信方法。

34. 上記生成ステップは、

作成者識別データを含む上記データを上記鍵データで暗号化すると共に、上記作成者識別データを含む上記取扱方針データを生成する

ことを特徴とする請求の範囲第 33 項に記載の情報送信方法。

35. 上記生成ステップは、

上記暗号化されたデータ及び上記取扱方針データに対する署名を生成することを特徴とする請求の範囲第33項に記載の情報送信方法。

36. 上記生成ステップは、

上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成することを特徴とする請求の範囲第33項に記載の情報送信方法。

37. 上記生成ステップは、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を生成することを特徴とする請求の範囲第33項に記載の情報送信方法。

38. 上記生成ステップは、

上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名を生成することを特徴とする請求の範囲第33項に記載の情報送信方法。

39. 上記生成ステップは、

上記取扱方針データに対する取扱方針用署名を生成し、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成することを特徴とする請求の範囲第33項に記載の情報送信方法。

40. 上記生成ステップは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化鍵データに対する鍵データ用署名を生成し、



上記送信ステップは、  
上記生成された鍵データ用署名を上記データ受信装置に送信する  
ことを特徴とする請求の範囲第 3 3 項、第 3 4 項、第 3 5 項、第 3 6 項、第 3  
8 項又は第 3 9 項に記載の情報送信方法。

4 1. 上記生成ステップは、  
上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データ  
を保存し、上記暗号化されたデータ、上記暗号化鍵データ及び上記取扱方針に対  
するセキュアコンテナ用署名の生成を行い、  
上記送信ステップは、  
上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記  
セキュアコンテナ用署名を上記データ受信装置に送信する  
ことを特徴とする請求の範囲第 3 7 項に記載の情報送信方法。

4 2. データ送信装置から送信された所定のデータを受信する情報受信方法にお  
いて、  
上記データ送信装置から送信された、所定の鍵データで暗号化された上記デー  
タと、当該データの取り扱い方針を記述した取扱方針データと、上記暗号化され  
たデータ及び上記取扱方針データの送信用の署名とを受信する受信ステップと、  
受信した上記署名の検証を行う検証ステップと  
を具えることを特徴とする情報受信方法。

4 3. 上記検証ステップは、  
上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成  
者識別データとを比較する  
ことを特徴とする請求の範囲第 4 2 項に記載の情報受信方法。

4 4. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データに対する署名を受信し、

上記検証ステップは、

上記暗号化されたデータ及び上記取扱方針データに対する署名の検証を行うことを特徴とする請求の範囲第 4 2 項に記載の情報受信方法。

4 5. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データ毎の署名を受信し、

上記検証ステップは、

上記暗号化されたデータ及び上記取扱方針データ毎の署名の検証を行うことを特徴とする請求の範囲第 4 2 項に記載の情報受信方法。

4 6. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を受信し、

上記検証ステップは、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第 4 2 項に記載の情報受信方法。

4 7. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータに対するデータ用署名と、上記取扱方針データ及び上記データ用署名に対する取扱方針用署名とを受信し、

上記検証ステップは、

上記データ用署名と、上記取扱方針用署名との検証を行う

ことを特徴とする請求の範囲第42項に記載の情報受信方法。

48. 上記受信ステップは、

上記データ送信装置から送信された、上記取扱方針データに対する取扱方針用署名と、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名とを受信し、

上記検証ステップは、

上記取扱方針用署名と、上記データ用署名との検証を行う

ことを特徴とする請求の範囲第42項に記載の情報受信方法。

49. 上記受信ステップは、

上記データ送信装置から送信された、配送鍵で暗号化された上記鍵データに対する鍵データ用署名を受信し、

上記検証ステップは、

上記鍵データ用署名の検証を行う

ことを特徴とする請求の範囲第42項、第43項、第44項、第45項、第47項又は第48項に記載の情報受信方法。

50. 上記受信ステップは、

上記データ送信装置から送信された、配送鍵で暗号化された上記鍵データ、上記暗号化されたデータ及び上記取扱方針に対するセキュアコンテナ用署名を受信し、

上記検証ステップは、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第46項に記載の情報受信方法。

51. 所定のデータを所定の鍵データで暗号化すると共に、上記データの取り扱

い方針を記述した取扱方針データを生成し、上記暗号化されたデータ及び上記取扱方針データの送信用の署名を生成する生成ステップと、

上記暗号化されたデータ及び上記取扱方針データと共に上記署名をデータ受信方法に送信する送信ステップと

を具えることを特徴とするプログラムを情報送信装置に実行させるプログラム格納媒体。

5 2. 上記生成ステップは、

作成者識別データを含む上記データを上記鍵データで暗号化すると共に、上記作成者識別データを含む上記取扱方針データを生成する

ことを特徴とする請求の範囲第 5 1 項に記載のプログラム格納媒体。

5 3. 上記生成ステップは、

上記暗号化されたデータ及び上記取扱方針データに対する署名を生成することを特徴とする請求の範囲第 5 1 項に記載のプログラム格納媒体。

5 4. 上記生成ステップは、

上記暗号化されたデータ及び上記取扱方針データに対する署名を別々に生成する

ことを特徴とする請求の範囲第 5 1 項に記載のプログラム格納媒体。

5 5. 上記生成ステップは、

上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を生成する

ことを特徴とする請求の範囲第 5 1 項に記載のプログラム格納媒体。

5 6. 上記生成ステップは、

上記暗号化されたデータに対するデータ用署名を生成すると共に上記取扱方針データ及び上記データ用署名に対する取扱方針用署名を生成することを特徴とする請求の範囲第51項に記載のプログラム格納媒体。

57. 上記生成ステップは、

上記取扱方針データに対する取扱方針用署名を生成し、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を生成することを特徴とする請求の範囲第51項に記載のプログラム格納媒体。

58. 上記生成ステップは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化鍵データに対する鍵データ用署名を生成し、

上記送信ステップは、

上記生成された鍵データ用署名を上記データ受信装置に送信する

ことを特徴とする請求の範囲第51項、第52項、第53項、第54項、第56項又は第57項に記載のプログラム格納媒体。

59. 上記生成ステップは、

上記データを暗号化するための鍵データを配送鍵で暗号化した暗号化鍵データを保存し、上記暗号化されたデータ、上記暗号化鍵データ及び上記取扱方針に対するセキュアコンテナ用署名の生成を行い、

上記送信ステップは、

上記暗号化されたデータ、上記暗号化鍵データ、上記取扱方針データ及び上記セキュアコンテナ用署名を上記データ受信装置に送信する

ことを特徴とする請求の範囲第55項に記載のプログラム格納媒体。

60. データ送信装置から送信された、所定の鍵データで暗号化された所定のデ

ータと、当該データの取り扱い方針を記述した取扱方針データと、上記暗号化されたデータ及び上記取扱方針データの送信用の署名とを受信する受信ステップと、

受信した上記署名の検証を行う検証ステップと  
を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

61. 上記検証ステップは、

上記データに含まれる作成者識別データと上記取扱方針データに含まれる作成者識別データとを比較する

ことを特徴とする請求の範囲第60項に記載のプログラム格納媒体。

62. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データに対する署名を受信し、

上記検証ステップは、

上記暗号化されたデータ及び上記取扱方針データに対する署名の検証を行う  
ことを特徴とする請求の範囲第60項に記載のプログラム格納媒体。

63. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データ毎の署名を受信し、

上記検証ステップは、

上記暗号化されたデータ及び上記取扱方針データ毎の署名の検証を行う  
ことを特徴とする請求の範囲第60項に記載のプログラム格納媒体。

64. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータ及び上記取扱方針データに対するセキュアコンテナ用署名を受信し、

上記検証ステップは、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第60項に記載のプログラム格納媒体。

65. 上記受信ステップは、

上記データ送信装置から送信された、上記暗号化されたデータに対するデータ用署名と、上記取扱方針データ及び上記データ用署名に対する取扱方針用署名を受信し、

上記検証ステップは、

上記データ用署名と、上記取扱方針用署名との検証を行う

ことを特徴とする請求の範囲第60項に記載のプログラム格納媒体。

66. 上記受信ステップは、

上記データ送信装置から送信された、上記取扱方針データに対する取扱方針用署名と、上記暗号化されたデータ及び上記取扱方針用署名に対するデータ用署名を受信し、

上記検証ステップは、

上記取扱方針用署名と、上記データ用署名との検証を行う

ことを特徴とする請求の範囲第60項に記載のプログラム格納媒体。

67. 上記受信ステップは、

上記データ送信装置から送信された、配送鍵で暗号化された上記鍵データに対する鍵データ用署名を受信し、

上記検証ステップは、

上記鍵データ用署名の検証を行う

ことを特徴とする請求の範囲第60項、第61項、第62項、第63項、第65項又は第66項に記載のプログラム格納媒体。

68. 上記受信ステップは、

上記データ送信装置から送信された、配送鍵で暗号化された上記鍵データ、上記暗号化されたデータ及び上記取扱方針に対するセキュアコンテナ用署名を受信し、

上記検証ステップは、

上記セキュアコンテナ用署名の検証を行う

ことを特徴とする請求の範囲第64項に記載のプログラム格納媒体。

69. 情報送信装置から所定のデータを情報受信装置に配信する情報配信システムにおいて、

上記情報送信装置は、

予め与えられている配送用の鍵データで暗号化された上記データを含む送信データを送信する送信手段を具え、

上記情報受信装置は、

上記送信データを受信する受信手段と、

予め与えられている上記鍵データを用いて上記データを復号する受信側制御手段とを具える

ことを特徴とする情報配信システム。

70. 情報送信装置から所定のデータを情報受信装置に配信する情報配信方法において、

上記情報送信装置により、予め与えられている配送用の鍵データで暗号化された上記データを含む送信データを送信する送信ステップと、

上記情報受信装置により、上記送信データを受信し、予め与えられている上記



鍵データを用いて上記データを復号する復号ステップと  
を具えることを特徴とする情報配信方法。

7 1. 所定のデータを情報受信装置に送信する情報送信装置において、  
上記情報受信装置に予め与えられている配送用の鍵データを用いて暗号化され  
た上記データを含む送信データを生成する送信側制御手段と、  
上記送信データを送信する送信手段と  
を具えることを特徴とする情報送信装置。

7 2. 上記送信側制御手段は、  
上記鍵データで暗号化された上記データとして、上記情報送信装置固有の個別  
鍵を含む送信データを生成する  
ことを特徴とする請求の範囲第 7 1 項に記載の情報送信装置。

7 3. 上記送信側制御手段は、  
定期的に更新される上記鍵データを用いて暗号化された上記データを含む送信  
データを生成する  
ことを特徴とする請求の範囲第 7 2 項に記載の情報送信装置。

7 4. 上記送信側制御手段は、  
予めまとめて与えられている複数の更新期間分の上記鍵データを用いて暗号化  
された上記データのうちの更新時期に応じた上記鍵データを用いて暗号化された  
上記データを含む上記送信データを生成する  
ことを特徴とする請求の範囲第 7 3 項に記載の情報送信装置。

7 5. 情報送信装置から送信された所定のデータを受信する情報受信装置におい  
て、

上記情報送信装置から送信された、配送用の鍵データで暗号化された上記データを含む送信データを受信する受信手段と、

予め与えられている上記鍵データを用いて上記データを復号する受信側制御手段と

を具えることを特徴とする情報受信装置。

76. 上記受信手段は、

上記鍵データで暗号化された上記データとして、上記情報受信装置固有の個別鍵を含む送信データを受信する

ことを特徴とする請求の範囲第75項に記載の情報受信装置。

77. 上記受信手段は、

定期的に更新される上記鍵データで暗号化された上記データを含む上記送信データを受信し、

上記受信側制御手段は、

定期的に更新されて与えられる上記鍵データを用いて上記データを復号することを特徴とする請求の範囲第76項に記載の情報受信装置。

78. 上記受信側制御手段は、

予めまとめて与えられている複数の更新期間分の上記鍵データのうちの更新時期に応じた上記鍵データを用いて上記データを復号する

ことを特徴とする請求の範囲第77項に記載の情報受信装置。

79. 所定のデータを情報受信装置に送信する情報送信方法において、

上記情報受信装置に予め与えられている配送用の鍵データを用いて暗号化された上記データを含む送信データを生成する生成ステップと、

上記送信データを送信する送信ステップと

を具えることを特徴とする情報送信方法。

80. 上記生成ステップは、

上記鍵データで暗号化された上記データとして、上記情報送信装置固有の個別鍵を含む送信データを生成する

ことを特徴とする請求の範囲第79項に記載の情報送信方法。

81. 上記生成ステップは、

定期的に更新される上記鍵データを用いて暗号化された上記データを含む送信データを生成する

ことを特徴とする請求の範囲第80項に記載の情報送信方法。

82. 上記生成ステップは、

予めまとめて与えられている複数の更新期間分の上記鍵データを用いて暗号化された上記データのうちの更新時期に応じた上記鍵データを用いて暗号化された上記データを含む上記送信データを生成する

ことを特徴とする請求の範囲第81項に記載の情報送信方法。

83. 情報送信装置から送信された所定のデータを受信する情報受信方法において、

上記情報送信装置から送信された、配送用の鍵データで暗号化された上記データを含む送信データを受信する受信ステップと、

予め与えられている上記鍵データを用いて上記データを復号する復号ステップと

を具えることを特徴とする情報受信方法。

84. 上記受信ステップは、

上記鍵データで暗号化された上記データとして、上記情報受信装置固有の個別鍵を含む送信データを受信する

ことを特徴とする請求の範囲第 8 3 項に記載の情報受信方法。

8 5. 上記受信ステップは、

定期的に更新される上記鍵データで暗号化された上記データを含む上記送信データを受信し、

上記復号ステップは、

定期的に更新されて与えられる上記鍵データを用いて上記データを復号することを特徴とする請求の範囲第 8 4 項に記載の情報受信方法。

8 6. 上記復号ステップは、

予めまとめて与えられている複数の更新期間分の上記鍵データのうちの更新時期に応じた上記鍵データを用いて上記データを復号する

ことを特徴とする請求の範囲第 8 5 項に記載の情報受信方法。

8 7. 情報受信装置に予め与えられている配送用の鍵データを用いて暗号化された所定のデータを含む送信データを生成する生成ステップと、

上記送信データを上記情報受信装置に送信する送信ステップと  
を具えることを特徴とするプログラムを情報送信装置に実行させるプログラム格納媒体。

8 8. 上記生成ステップは、

上記鍵データで暗号化された上記データとして、上記情報送信装置固有の個別鍵を含む送信データを生成する

ことを特徴とする請求の範囲第 8 7 項に記載のプログラム格納媒体。

89. 上記生成ステップは、

定期的に更新される上記鍵データを用いて暗号化された上記データを含む送信データを生成する

ことを特徴とする請求の範囲第88項に記載のプログラム格納媒体。

90. 上記生成ステップは、

予めまとめて与えられている複数の更新期間分の上記鍵データを用いて暗号化された上記データのうちの更新時期に応じた上記鍵データを用いて暗号化された上記データを含む上記送信データを生成する

ことを特徴とする請求の範囲第89項に記載のプログラム格納媒体。

91. 情報送信装置から送信された、配送用の鍵データで暗号化された所定のデータを含む送信データを受信する受信ステップと、

予め与えられている上記鍵データを用いて上記データを復号する復号ステップと

を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

92. 上記受信ステップは、

上記鍵データで暗号化された上記データとして、上記情報受信装置固有の個別鍵を含む送信データを受信する

ことを特徴とする請求の範囲第91項に記載のプログラム格納媒体。

93. 上記受信ステップは、

定期的に更新される上記鍵データで暗号化された上記データを含む上記送信データを受信し、

上記復号ステップは、

定期的に更新されて与えられる上記鍵データを用いて上記データを復号することを特徴とする請求の範囲第 9 2 項に記載のプログラム格納媒体。

9 4. 上記復号ステップは、

予めまとめて与えられている複数の更新期間分の上記鍵データのうちの更新時期に応じた上記鍵データを用いて上記データを復号する

ことを特徴とする請求の範囲第 9 3 項に記載のプログラム格納媒体。

9 5. 情報送信装置から所定のコンテンツデータを情報受信装置に配信する情報配信システムにおいて、

上記情報送信装置は、

上記コンテンツデータをコンテンツ鍵で暗号化すると共に、当該コンテンツ鍵を上記情報送信装置固有の個別鍵で暗号化する送信側制御手段と、

所定の配送鍵で上記個別鍵を暗号化してなる外部から供給される暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する送信手段とを具え、

上記情報受信装置は、

上記暗号化個別鍵と共に上記コンテンツ鍵で暗号化された上記コンテンツデータ及び上記個別鍵で暗号化された上記コンテンツ鍵を受信する受信手段と、

予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵で上記コンテンツデータを復号する受信側制御手段とを具える

ことを特徴とする情報配信システム。

9 6. 情報送信装置から所定のコンテンツデータを情報受信装置に配信する情報配信方法において、

上記情報送信装置により、上記コンテンツデータをコンテンツ鍵で暗号化する

と共に、当該コンテンツ鍵を上記情報送信装置固有の個別鍵で暗号化し、所定の配送鍵で上記個別鍵を暗号化してなる外部から供給される暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する送信ステップと、

上記情報受信装置により、上記暗号化個別鍵と共に上記コンテンツ鍵で暗号化された上記コンテンツデータ及び上記個別鍵で暗号化された上記コンテンツ鍵を受信し、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵で上記コンテンツデータを復号する復号ステップと

を具えることを特徴とする情報配信方法。

#### 97. 所定のコンテンツデータを情報受信装置に送信する情報送信装置において

上記コンテンツデータをコンテンツ鍵で暗号化すると共に、当該コンテンツ鍵を上記情報送信装置固有の個別鍵で暗号化する送信側制御手段と、

所定の配送鍵で上記個別鍵を暗号化してなる外部から供給される暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する送信手段と

を具えることを特徴とする情報送信装置。

#### 98. 上記送信側制御手段は、

上記暗号化個別鍵と共に外部から供給される上記個別鍵で上記コンテンツ鍵を暗号化する

ことを特徴とする請求の範囲第97項に記載の情報送信装置。

#### 99. 上記送信手段は、

定期的に更新される上記配送鍵で上記個別鍵を暗号化してなる外部から供給さ

れる上記暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信することを特徴とする請求の範囲第 9 8 項に記載の情報送信装置。

1 0 0. 上記送信手段は、

予めまとめて与えられている複数の更新期間分の上記暗号化個別鍵のうちの更新時期に応じた上記暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する

ことを特徴とする請求の範囲第 9 9 項に記載の情報送信装置。

1 0 1. 情報送信装置から送信される所定のコンテンツデータを受信する情報受信装置において、

上記情報送信装置から送信される、コンテンツ鍵で暗号化された上記コンテンツデータと、上記情報送信装置固有の個別鍵で暗号化された上記コンテンツ鍵と、所定の配送鍵で暗号化された上記個別鍵とを受信する受信手段と、

予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵で上記コンテンツデータを復号する受信側制御手段と

を具えることを特徴とする情報受信装置。

1 0 2. 上記受信側制御手段は、

定期的に更新される上記配送鍵で上記個別鍵を復号する

ことを特徴とする請求の範囲第 1 0 1 項に記載の情報受信装置。

1 0 3. 上記受信側制御手段は、

予めまとめて与えられている複数の更新期間分の上記配送鍵のうちの更新時期



に応じた上記配送鍵で上記個別鍵を復号する

ことを特徴とする請求の範囲第102項に記載の情報受信装置。

104. 所定のコンテンツデータを情報受信装置に送信する情報送信方法において、

上記コンテンツデータをコンテンツ鍵で暗号化すると共に、当該コンテンツ鍵を上記情報送信装置固有の個別鍵で暗号化する暗号化ステップと、

所定の配送鍵で上記個別鍵を暗号化してなる外部から供給される暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する送信ステップと、

を具えることを特徴とする情報送信方法。

105. 上記暗号化ステップは、

上記暗号化個別鍵と共に外部から供給される上記個別鍵で上記コンテンツ鍵を暗号化する

ことを特徴とする請求の範囲第104項に記載の情報送信方法。

106. 上記送信ステップは、

定期的に更新される上記配送鍵で上記個別鍵を暗号化してなる外部から供給される上記暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する

ことを特徴とする請求の範囲第105項に記載の情報送信方法。

107. 上記送信ステップは、

予めまとめて与えられている複数の更新期間分の上記暗号化個別鍵のうちの更新時期に応じた上記暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送

信する

ことを特徴とする請求の範囲第106項に記載の情報送信方法。

108. 情報送信装置から送信される所定のコンテンツデータを受信する情報受信方法において、

上記情報送信装置から送信される、コンテンツ鍵で暗号化された上記コンテンツデータと、上記情報送信装置固有の個別鍵で暗号化された上記コンテンツ鍵と、所定の配送鍵で暗号化された上記個別鍵とを受信する受信ステップと、

予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵で上記コンテンツデータを復号する復号ステップと

を具えることを特徴とする情報受信方法。

109. 上記復号ステップは、

定期的に更新される上記配送鍵で上記個別鍵を復号する

ことを特徴とする請求の範囲第108項に記載の情報受信方法。

110. 上記復号ステップは、

予めまとめて与えられている複数の更新期間分の上記配送鍵のうちの更新時期に応じた上記配送鍵で上記個別鍵を復号する

ことを特徴とする請求の範囲第109項に記載の情報受信方法。

111. 所定のコンテンツデータをコンテンツ鍵で暗号化すると共に、当該コンテンツ鍵を情報送信装置固有の個別鍵で暗号化する暗号化ステップと、

所定の配送鍵で上記個別鍵を暗号化してなる外部から供給される暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する送信ステップと、

を具えることを特徴とするプログラムを情報送信装置に実行させるプログラム格納媒体。

1 1 2. 上記暗号化ステップは、

上記暗号化個別鍵と共に外部から供給される上記個別鍵で上記コンテンツ鍵を暗号化する

ことを特徴とする請求の範囲第 1 1 1 項に記載のプログラム格納媒体。

1 1 3. 上記送信ステップは、

定期的に更新される上記配信鍵で上記個別鍵を暗号化してなる外部から供給される上記暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する

ことを特徴とする請求の範囲第 1 1 2 項に記載のプログラム格納媒体。

1 1 4. 上記送信ステップは、

予めまとめて与えられている複数の更新期間分の上記暗号化個別鍵のうちの更新時期に応じた上記暗号化個別鍵を上記コンテンツ鍵で暗号化した上記コンテンツデータ及び上記個別鍵で暗号化したコンテンツ鍵と共に上記情報受信装置に送信する

ことを特徴とする請求の範囲第 1 1 3 項に記載のプログラム格納媒体。

1 1 5. 情報送信装置から送信される、コンテンツ鍵で暗号化された所定のコンテンツデータと、上記情報送信装置固有の個別鍵で暗号化された上記コンテンツ鍵と、所定の配信鍵で暗号化された上記個別鍵とを受信する受信ステップと、

予め与えられている上記配信鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵で上記コンテンツデータを復号する復号ステップと

を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

1 1 6. 上記復号ステップは、

定期的に更新される上記配送鍵で上記個別鍵を復号すること  
ことを特徴とする請求の範囲第 1 1 5 項に記載のプログラム格納媒体。

1 1 7. 上記復号ステップは、

予めまとめて与えられている複数の更新期間分の上記配送鍵のうちの更新時期に応じた上記配送鍵で上記個別鍵を復号する

ことを特徴とする請求の範囲第 1 1 6 項に記載のプログラム格納媒体。

1 1 8. 情報送信装置から情報受信装置に対して所定のコンテンツ鍵で暗号化されたコンテンツデータを配信する情報配信システムにおいて、

上記情報受信装置は、

上記コンテンツデータの利用権と、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵とを有し、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成する受信側制御手段と、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信することにより、上記他の機器に上記コンテンツを再生させる送信手段と

を具えることを特徴とする情報配信システム。

1 1 9. 上記送信手段は、

上記コンテンツデータを上記他の機器に送信し、

上記他の機器は、

上記情報受信装置から上記コンテンツ鍵で暗号化された上記コンテンツデータ

を受け取り、当該受け取ったコンテンツデータを上記コンテンツ鍵及び上記再生コマンドを用いて再生する

ことを特徴とする請求の範囲第 1 1 8 項に記載の情報配信システム。

1 2 0. 上記受信側制御手段は、

上記他の機器との間で、上記コンテンツデータの利用に際しての登録可否を表す登録情報を相互に検査し合い、

上記送信手段は、

上記受信側制御手段による上記登録情報の検査結果が互いに利用可である場合に上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求の範囲第 1 1 9 項に記載の情報配信システム。

1 2 1. 情報送信装置から情報受信装置に対して所定のコンテンツ鍵で暗号化されたコンテンツデータを配信する情報配信方法において、

上記コンテンツデータの利用権と、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵とを有する上記情報受信装置により、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成する生成ステップと、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する送信ステップと

を具備することを特徴とする情報配信方法。

1 2 2. 上記送信ステップは、

上記コンテンツデータを上記他の機器に送信し、

上記他の機器により、上記情報受信装置から上記コンテンツ鍵で暗号化された上記コンテンツデータを受け取り、当該受け取ったコンテンツデータを上記コンテンツ鍵及び上記再生コマンドを用いて再生する再生ステップ

を具えることを特徴とする請求の範囲第 1 2 1 項に記載の情報配信方法。

1 2 3. 上記生成ステップは、

上記他の機器との間で、上記コンテンツデータの利用に際しての登録可否を表す登録情報を相互に検査し合い、

上記送信ステップは、

上記登録情報の検査結果が互いに利用可である場合に上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求の範囲第 1 2 2 項に記載の情報配信方法。

1 2 4. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置において、

上記コンテンツデータの利用権を有する場合に、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵を有し、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成する受信側制御手段と、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する送信手段とを具えることを特徴とする情報受信装置。

1 2 5. 上記受信側制御手段は、

上記他の機器の上記コンテンツデータの利用に際しての登録可否を表す登録情報を検査し、

上記送信手段は、

上記受信側制御手段による上記登録情報の検査結果が利用可である場合に上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求の範囲第 1 2 4 項に記載の情報受信装置。

1 2 6. 上記受信側制御手段は、

上記他の機器で再生させる上記コンテンツデータの識別情報を含む上記再生コマンドを生成する

ことを特徴とする請求の範囲第 1 2 5 項に記載の情報受信装置。

1 2 7. 上記受信側制御手段は、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器と共有している一時鍵で暗号化し、

上記送信手段は、

上記一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する

ことを特徴とする請求の範囲第 1 2 6 項に記載の情報受信装置。

1 2 8. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置と通信し得る機器において、

上記コンテンツデータの利用権を持たない場合、上記コンテンツデータの利用権と、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵とを有する上記情報受信装置から送信される再生コマンドと、上記コンテンツ鍵とを受信すると共に、上記情報受信装置から送信される上記コンテンツデータを受信する受信手段と、

上記コンテンツデータを上記再生コマンド及び上記コンテンツ鍵を用いて再生する機器側制御手段と

を具備することを特徴とする機器。

1 2 9. 上記機器側制御手段は、

上記情報受信装置の上記コンテンツデータの利用に際しての登録可否を表す登録情報を検査し、

上記受信手段は、

上記機器側制御手段による上記登録情報の検査結果が利用可である場合に上記コンテンツ鍵及び上記再生コマンドを受信することを特徴とする請求の範囲第128項に記載の機器。

130. 上記受信手段は、

上記情報受信装置から送信される再生対象の上記コンテンツデータの識別情報を含む上記再生コマンドを受信することを特徴とする請求の範囲第129項に記載の機器。

131. 上記受信手段は、

上記情報受信装置と共有している一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を受信し、

上記機器側制御手段は、

上記一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を上記一時鍵で復号して用いる

ことを特徴とする請求の範囲第130項に記載の機器。

132. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置から他の機器に所定の情報を送信する送信方法において、

上記コンテンツデータの利用権と、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵とを有する場合に、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成する生成ステップと、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する送信ステップと



を具えることを特徴とする情報受信装置の送信方法。

1 3 3. 上記生成ステップは、

上記他の機器の上記コンテンツデータの利用に際しての登録可否を表す登録情報を検査し、

上記送信ステップは、

上記受信側制御手段による上記登録情報の検査結果が利用可である場合に上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求の範囲第 1 3 2 項に記載の情報受信装置の送信方法。

1 3 4. 上記生成ステップは、

上記他の機器で再生させる上記コンテンツデータの識別情報を含む上記再生コマンドを生成する

ことを特徴とする請求の範囲第 1 3 3 項に記載の情報受信装置の送信方法。

1 3 5. 上記生成ステップは、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器と共有している一時鍵で暗号化し、

上記送信ステップは、

上記一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する

ことを特徴とする請求の範囲第 1 3 4 項に記載の情報受信装置の送信方法。

1 3 6. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置と通信し得る機器の再生方法において、

上記コンテンツデータの利用権を持たない場合、上記コンテンツデータの利用権と、上記情報送信装置から配信される上記コンテンツデータを復号するための

上記コンテンツ鍵とを有する上記情報受信装置から送信される再生コマンドと、  
上記コンテンツ鍵とを受信すると共に、上記情報受信装置から送信される上記コ  
ンテンツデータを受信する受信ステップと、

上記コンテンツデータを上記再生コマンド及び上記コンテンツ鍵を用いて再生  
する再生ステップと

を具えることを特徴とする機器の再生方法。

137. 上記受信ステップは、

上記情報受信装置の上記コンテンツデータの利用に際しての登録可否を表す登  
録情報を検査し、当該登録情報の検査結果が利用可である場合に上記情報受信装  
置から送信される上記コンテンツ鍵及び上記再生コマンドを受信する

ことを特徴とする請求の範囲第136項に記載の機器の再生方法。

138. 上記受信ステップは、

上記情報受信装置から送信される再生対象の上記コンテンツデータの識別情報  
を含む上記再生コマンドを受信する

ことを特徴とする請求の範囲第139項に記載の機器の再生方法。

139. 上記受信ステップは、

上記情報受信装置と共有している一時鍵で暗号化された上記再生コマンド及び  
上記コンテンツ鍵を受信し、

上記再生ステップは、

上記一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を上記一時  
鍵で復号して用いる

ことを特徴とする請求の範囲第138項に記載の機器の再生方法。

140. 所定のコンテンツデータの利用権と、情報送信装置から所定のコンテン

ッ鍵で暗号化されて配信される上記コンテンツデータを復号するための上記コンテンツ鍵とを有する場合に、上記コンテンツデータの利用権を持たない他の機器に対する再生コマンドを生成する生成ステップと、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する送信ステップと

を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

1 4 1. 上記生成ステップは、

上記他の機器の上記コンテンツデータの利用に際しての登録可否を表す登録情報を検査し、

上記送信ステップは、

上記受信側制御手段による上記登録情報の検査結果が利用可である場合に上記他の機器に対して上記コンテンツ鍵及び上記再生コマンドを送信する

ことを特徴とする請求の範囲第 1 4 0 項に記載のプログラム格納媒体。

1 4 2. 上記生成ステップは、

上記他の機器で再生させる上記コンテンツデータの識別情報を含む上記再生コマンドを生成する

ことを特徴とする請求の範囲第 1 4 1 項に記載のプログラム格納媒体。

1 4 3. 上記生成ステップは、

上記再生コマンド及び上記コンテンツ鍵を上記他の機器と共有している一時鍵で暗号化し、

上記送信ステップは、

上記一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を上記他の機器に送信する

ことを特徴とする請求の範囲第142項に記載のプログラム格納媒体。

144. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置と通信し得る機器の再生方法において、

所定のコンテンツデータの利用権を持たない場合、上記コンテンツデータの利用権と、上記情報送信装置から配信される上記コンテンツデータを復号するための上記コンテンツ鍵とを有する上記情報受信装置から送信される再生コマンドと、上記コンテンツ鍵とを受信すると共に、上記情報受信装置から送信される上記コンテンツデータを受信する受信ステップと、

上記コンテンツデータを上記再生コマンド及び上記コンテンツ鍵を用いて再生する再生ステップと

を具えることを特徴とするプログラムを情報受信装置と通信し得る機器に実行させるプログラム格納媒体。

145. 上記受信ステップは、

上記情報受信装置の上記コンテンツデータの利用に際しての登録可否を表す登録情報を検査し、当該登録情報の検査結果が利用可である場合に上記情報受信装置から送信される上記コンテンツ鍵及び上記再生コマンドを受信する

ことを特徴とする請求の範囲第144項に記載のプログラム格納媒体。

146. 上記受信ステップは、

上記情報受信装置から送信される再生対象の上記コンテンツデータの識別情報を含む上記再生コマンドを受信する

ことを特徴とする請求の範囲第145項に記載のプログラム格納媒体。

147. 上記受信ステップは、

上記情報受信装置と共有している一時鍵で暗号化された上記再生コマンド及び

上記コンテンツ鍵を受信し、

上記再生ステップは、

上記一時鍵で暗号化された上記再生コマンド及び上記コンテンツ鍵を上記一時鍵で復号して用いる

ことを特徴とする請求の範囲第 1 4 6 項に記載のプログラム格納媒体。

1 4 8. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを情報受信装置に送信する情報配信システムにおいて、

上記情報送信装置は、

上記情報送信装置固有の個別鍵で上記コンテンツ鍵を暗号化する送信側制御手段と、

少なくとも上記個別鍵で暗号化された上記コンテンツ鍵と、所定の周期で更新される配信鍵で上記個別鍵を暗号化してなる外部から供給された暗号化個別鍵とを上記情報受信装置に送信する送信手段とを具え、

上記情報受信装置は、

少なくとも上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを受信する受信手段と、

上記配信鍵が更新される前に、予め与えられている上記配信鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存することにより、上記配信鍵が更新された後に上記コンテンツ鍵を復号可能とする受信側制御手段とを具える

ことを特徴とする情報配信システム。

1 4 9. 情報送信装置から所定のコンテンツ鍵で暗号化されたコンテンツデータを情報受信装置に送信する情報配信方法において、

上記情報送信装置により、当該情報送信装置固有の個別鍵で上記コンテンツ鍵を暗号化し、少なくとも上記個別鍵で暗号化された上記コンテンツ鍵と、所定の

周期で更新される配送鍵で上記個別鍵を暗号化してなる外部から供給された暗号化個別鍵とを上記情報受信装置に送信する送信ステップと、

上記情報受信装置により、少なくとも上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを受信し、上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存することにより、上記配送鍵が更新された後に上記コンテンツを復号可能とする保存ステップとを具えることを特徴とする情報配信方法。

150. 情報送信装置から配信されるコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信装置において、

上記情報送信装置から送信される少なくとも、個別鍵で暗号化された上記コンテンツ鍵と、所定の周期で更新される配送鍵で上記個別鍵を暗号化してなる暗号化個別鍵とを上記配送鍵が更新される前に受信する受信手段と、

上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存することにより、上記配送鍵が更新された後に上記コンテンツを復号可能とする制御手段と

を具えることを特徴とする情報受信装置。

151. 上記受信手段は、

上記情報送信装置固有の上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを上記配送鍵が更新される前に受信することを特徴とする請求の範囲第150項に記載の情報受信装置。

152. 上記制御手段は、

上記更新前の上記配送鍵を用いて復号した上記コンテンツ鍵を保存鍵で暗号化

して保存する

ことを特徴とする請求の範囲第151項に記載の情報受信装置。

153. 上記制御手段は、

上記更新前の上記配送鍵を用いて復号した上記コンテンツ鍵を上記情報受信装置固有の上記保存鍵で暗号化して保存する

ことを特徴とする請求の範囲第152項に記載の情報受信装置。

154. 上記受信手段は、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを送信用の署名と共に受信し、

上記制御手段は、

上記署名を検証し、上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とが改竄されていないことを確認した場合、上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存する

ことを特徴とする請求の範囲第153項に記載の情報受信装置。

155. 上記受信手段は、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを当該上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とに別々に付加された署名と共に受信する

ことを特徴とする請求の範囲第154項に記載の情報受信装置。

156. 上記受信手段は、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを当該上記個別鍵で暗号化された上記コンテンツ鍵と、

上記暗号化個別鍵との全体に対して付加された署名と共に受信することを特徴とする請求の範囲第 1 5 5 項に記載の情報受信装置。

1 5 7. 情報送信装置から配信されるコンテンツ鍵で暗号化されたコンテンツデータを受信する情報受信方法において、

上記情報送信装置から送信される少なくとも、個別鍵で暗号化された上記コンテンツ鍵と、所定の周期で更新される配送鍵で上記個別鍵を暗号化してなる暗号化個別鍵とを上記配送鍵が更新される前に受信する受信ステップと、

上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存することにより、上記配送鍵が更新された後に上記コンテンツを復号可能とする保存ステップと、

を具えることを特徴とする情報受信方法。

1 5 8. 上記受信ステップは、

上記情報送信装置固有の上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを上記配送鍵が更新される前に受信する

ことを特徴とする請求の範囲第 1 5 7 項に記載の情報受信方法。

1 5 9. 上記保存ステップは、

上記更新前の上記配送鍵を用いて復号した上記コンテンツ鍵を保存鍵で暗号化して保存する

ことを特徴とする請求の範囲第 1 5 8 項に記載の情報受信方法。

1 6 0. 上記保存ステップは、

上記更新前の上記配送鍵を用いて復号した上記コンテンツ鍵を情報受信装置固有の上記保存鍵で暗号化して保存する



ことを特徴とする請求の範囲第 1 5 9 項に記載の情報受信方法。

1 6 1. 上記受信ステップは、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを送信用の署名と共に受信し、

上記保存ステップは、

上記署名を検証し、上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とが改竄されていないことを確認した場合、上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存する

ことを特徴とする請求の範囲第 1 6 0 項に記載の情報受信方法。

1 6 2. 上記受信ステップは、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを当該上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とに別々に付加された署名と共に受信する

ことを特徴とする請求の範囲第 1 6 1 項に記載の情報受信方法。

1 6 3. 上記受信ステップは、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを当該上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵との全体に対して付加された署名と共に受信する

ことを特徴とする請求の範囲第 1 6 2 項に記載の情報受信方法。

1 6 4. コンテンツ鍵で暗号化されたコンテンツデータを送信する情報送信装置から送信される少なくとも、個別鍵で暗号化された上記コンテンツ鍵と、所定の周期で更新される配送鍵で上記個別鍵を暗号化してなる暗号化個別鍵とを上記配

送鍵が更新される前に受信する受信ステップと、

上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存することにより、上記配送鍵が更新された後に上記コンテンツを復号可能とする保存ステップと、

を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

165. 上記受信ステップは、

上記情報送信装置固有の上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを上記配送鍵が更新される前に受信する

ことを特徴とする請求の範囲第164項に記載のプログラム格納媒体。

166. 上記保存ステップは、

上記更新前の上記配送鍵を用いて復号した上記コンテンツ鍵を保存鍵で暗号化して保存する

ことを特徴とする請求の範囲第165項に記載のプログラム格納媒体。

167. 上記保存ステップは、

上記更新前の上記配送鍵を用いて復号した上記コンテンツ鍵を情報受信装置固有の上記保存鍵で暗号化して保存する

ことを特徴とする請求の範囲第166項に記載のプログラム格納媒体。

168. 上記受信ステップは、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを送信用の署名と共に受信し、

上記保存ステップは、

上記署名を検証し、上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とが改竄されていないことを確認した場合、上記配送鍵が更新される前に、予め与えられている上記配送鍵で上記個別鍵を復号し、当該復号された個別鍵で上記コンテンツ鍵を復号し、当該復号されたコンテンツ鍵を保存することを特徴とする請求の範囲第 1 6 7 項に記載のプログラム格納媒体。

1 6 9. 上記受信ステップは、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを当該上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とに別々に付加された署名と共に受信することを特徴とする請求の範囲第 1 6 8 項に記載のプログラム格納媒体。

1 7 0. 上記受信ステップは、

上記情報送信装置から送信される上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵とを当該上記個別鍵で暗号化された上記コンテンツ鍵と、上記暗号化個別鍵との全体に対して付加された署名と共に受信することを特徴とする請求の範囲第 1 6 9 項に記載のプログラム格納媒体。

1 7 1. 情報送信装置から配信されるコンテンツデータを第 1 及び第 2 の情報受信装置で受信する情報受信システムにおいて、

上記コンテンツデータの利用権を有する上記第 1 の情報受信装置は、

上記コンテンツデータを利用するための登録情報が異なる上記第 2 の情報受信装置に上記第 1 の情報受信装置の第 1 の登録情報を送信する第 1 の送信手段と、

上記第 2 の情報受信装置の第 2 の登録情報を受信する第 1 の受信手段と、

上記第 2 の登録情報により上記第 2 の情報受信装置に対する上記コンテンツデータの利用可否を判断する第 1 の制御手段とを具え、

上記第 2 の情報受信装置は、

上記第 1 の情報受信装置に上記第 2 の登録情報を送信する第 2 の送信手段と、  
上記第 1 の情報受信装置の上記第 1 の登録情報を受信する第 2 の受信手段と、  
上記第 2 の登録情報により上記第 1 の情報受信装置に対する上記コンテンツデ  
ータの利用可否を判断する第 2 の制御手段とを具え、

上記第 1 及び第 2 の情報受信装置は、上記第 1 及び第 2 の制御手段により上記  
コンテンツデータの利用可否を相互に判断し、上記第 1 及び第 2 の情報受信装置  
が共に上記コンテンツデータを利用可と判断した場合、上記第 1 の情報受信装置  
の上記第 1 の送信手段から上記第 2 の情報受信装置に上記利用権を送信して引き  
渡すことにより上記第 2 の情報受信装置で上記コンテンツデータを利用可能とす  
る

ことを特徴とする情報受信システム。

172. 上記第 1 の情報受信装置の上記第 1 の制御手段は、

上記コンテンツデータを利用可と判断した上記第 2 の情報受信装置で利用する  
上記コンテンツデータの利用分の課金情報を生成して保持する

ことを特徴とする請求の範囲第 171 項に記載の情報受信システム。

173. 上記第 2 の情報受信装置の上記第 2 の制御手段は、

上記コンテンツデータの利用分の課金情報を生成して保持する

ことを特徴とする請求の範囲第 171 項に記載の情報受信システム。

174. 情報送信装置から配信されるコンテンツデータを利用するための登録情  
報が異なる複数の上記情報受信装置間で上記登録情報を授受することにより上記  
複数の情報受信装置間で上記コンテンツデータの利用可否を相互に判断する判断  
ステップと、

上記複数の情報受信装置のうちの上記コンテンツデータの利用権を有する第 1  
の情報受信装置が上記コンテンツデータの利用可と判断した第 2 の情報受信装置

に対して上記利用権を引き渡すことにより、上記利用権が引き渡された上記第 2 の情報受信装置で上記コンテンツデータを利用可能とする引渡ステップと  
を具えることを特徴とするコンテンツの利用方法。

175. 上記コンテンツデータの利用権を有する上記第 1 の情報受信装置は、上記コンテンツデータの利用可と判断した上記第 2 の情報受信装置で利用する上記コンテンツデータの利用分の課金情報を生成して保持する保持ステップ  
を具えることを特徴とする請求の範囲第 174 項に記載のコンテンツの利用方法。

176. 上記コンテンツデータの利用権を受け取った上記第 2 の情報受信装置は、上記コンテンツデータの利用分の課金情報を生成して保持する保持ステップ  
を具えることを特徴とする請求の範囲第 174 項に記載のコンテンツの利用方法。

177. 情報送信装置から配信されるコンテンツデータを受信する情報受信装置において、

上記コンテンツデータを利用するための登録情報が異なる他の情報受信装置に自己の第 1 の登録情報を送信する送信手段と、

上記他の情報受信装置の第 2 の登録情報を受信する受信手段と、

上記第 1 及び第 2 の登録情報により上記他の情報受信装置との間で上記コンテンツデータの利用可否を相互に判断する制御手段と

を具え、上記コンテンツデータの利用権を有する場合に、上記制御手段は上記コンテンツデータの利用可であると判断された上記他の情報受信装置に対して上記送信手段を介して上記利用権を引き渡すことにより、上記利用権が引き渡された上記他の情報受信装置で上記コンテンツデータを利用可能とする

ことを特徴とする情報受信装置。

178. 上記制御手段は、

上記コンテンツデータの利用権を引き渡した上記他の情報受信装置で利用する  
上記コンテンツデータの利用分の課金情報を生成して保持する  
ことを特徴とする請求の範囲第177項に記載の情報受信装置。

179. 上記制御手段は、

所定のコンテンツ鍵で暗号化された上記コンテンツデータと、上記コンテンツ  
鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報と  
を保持し、上記取扱方針データ及び上記価格情報に基づいて上記課金情報を生成  
して保持する

ことを特徴とする請求の範囲第178項に記載の情報受信装置。

180. 上記制御手段は、

上記取扱方針データ及び上記価格情報に基づいて上記コンテンツデータの利用  
権を記述した使用許諾条件情報を生成し、

上記送信手段は、

上記他の情報受信装置に上記コンテンツデータの利用権として、上記使用許諾  
条件情報を送信する

ことを特徴とする請求の範囲第179項に記載の情報受信装置。

181. 上記制御手段は、

上記コンテンツ鍵を上記他の情報受信装置との間で共有している一時鍵で暗号  
化し、

上記送信手段は、

上記他の情報受信装置に上記使用許諾条件情報と共に、上記コンテンツ鍵で暗  
号化された上記コンテンツデータと、上記一時鍵で暗号化された上記コンテンツ

鍵とを送信する

ことを特徴とする請求の範囲第180項に記載の情報受信装置。

182. 上記制御手段は、

所定のコンテンツ鍵で暗号化された上記コンテンツデータと、上記コンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とを保持し、

上記送信手段は、

上記他の情報受信装置に上記コンテンツデータの利用権を記述する使用許諾条件情報と、上記コンテンツデータの利用分の課金情報とを生成するための上記取扱方針データ及び上記価格情報を送信する

ことを特徴とする請求の範囲第177項に記載の情報受信装置。

183. 上記制御手段は、

上記コンテンツ鍵を上記他の情報受信装置との間で共有している一時鍵で暗号化し、

上記送信手段は、

上記他の情報受信装置に上記取扱方針データ及び上記価格情報と共に、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記一時鍵で暗号化された上記コンテンツ鍵とを送信する

ことを特徴とする請求の範囲第182項に記載の情報受信装置。

184. 情報送信装置から配信されるコンテンツデータを受信する情報受信装置において、

上記コンテンツデータを利用するための登録情報が異なる他の情報受信装置に自己の第1の登録情報を送信する送信手段と、

上記他の情報受信装置の第2の登録情報を受信する受信手段と、

上記第 1 及び第 2 の登録情報により上記他の情報受信装置との間で上記コンテンツデータの利用可否を相互に判断する制御手段と

を具え、上記コンテンツデータの利用権を有しない場合に、上記コンテンツデータの利用可であると判断された上記他の情報受信装置のうち、上記コンテンツデータの利用権を有する情報受信装置から送信される上記利用権を上記受信手段によって受信して上記コンテンツデータを利用可能とする

ことを特徴とする情報受信装置。

1 8 5. 上記制御手段は、

上記コンテンツデータの利用分の課金情報を生成して保持することを特徴とする請求の範囲第 1 8 4 項に記載の情報受信装置。

1 8 6. 上記受信手段は、

上記コンテンツデータの利用権を有する情報受信装置から送信される、上記コンテンツデータを暗号化している所定のコンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とを受信し、

上記制御手段は、

上記取扱方針データ及び上記価格情報に基づいて上記課金情報を生成して保持する

ことを特徴とする請求の範囲第 1 8 5 項に記載の情報受信装置。

1 8 7. 上記制御手段は、

上記取扱方針データ及び上記価格情報に基づいて上記コンテンツデータの利用権を記述した使用許諾条件情報を生成して保持する

ことを特徴とする請求の範囲第 1 8 6 項に記載の情報受信装置。

1 8 8. 上記受信手段は、



上記コンテンツデータの利用権を有する情報受信装置から送信される、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記他の情報受信装置との間で共有している一時鍵で暗号化された上記コンテンツ鍵とを受信し、

上記送信手段は、

上記コンテンツ鍵を上記一時鍵で復号し、当該復号した上記コンテンツ鍵を自己固有の保存鍵で暗号化して保存すると共に、上記コンテンツ鍵で暗号化された上記コンテンツデータを保持する

ことを特徴とする請求の範囲第 187 項に記載の情報受信装置。

189. 情報送信装置から配信されるコンテンツデータを受信する情報受信装置のコンテンツの利用方法において、

上記コンテンツデータを利用するための登録情報が異なる他の情報受信装置との間で上記登録情報を授受する授受ステップと、

上記登録情報により上記他の情報受信装置との間で上記コンテンツデータの利用可否を相互に判断する判断ステップと、

上記コンテンツデータの利用権を有する場合に、上記コンテンツデータの利用可であると判断された上記他の情報受信装置に対して上記利用権を引き渡すことにより、上記利用権が引き渡された上記他の情報受信装置で上記コンテンツデータを利用可能とする引渡ステップと

を具えることを特徴とするコンテンツの利用方法。

190. 上記コンテンツデータの利用権を引き渡した上記他の情報受信装置で利用する上記コンテンツデータの利用分の課金情報を生成して保持する生成保持ステップ

を具えることを特徴とする請求の範囲第 189 項に記載のコンテンツの利用方法。

191. 上記生成保持ステップは、

所定のコンテンツ鍵で暗号化された上記コンテンツデータと共に保持している上記コンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とに基づいて上記課金情報を生成して保持する

ことを特徴とする請求の範囲第190項に記載のコンテンツの利用方法。

192. 上記取扱方針データ及び上記価格情報に基づいて上記コンテンツデータの利用権を記述した使用許諾条件情報を生成する生成ステップを具え、

上記引渡ステップは、

上記他の情報受信装置に上記コンテンツデータの利用権として、上記使用許諾条件情報を引き渡す

ことを特徴とする請求の範囲第191項に記載のコンテンツの利用方法。

193. 上記コンテンツ鍵を上記他の情報受信装置との間で共有している一時鍵で暗号化する暗号化ステップを具え、

上記引渡ステップは、

上記他の情報受信装置に上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記一時鍵で暗号化された上記コンテンツ鍵とを送信する

ことを特徴とする請求の範囲第192項に記載のコンテンツの利用方法。

194. 上記引渡ステップは、

所定のコンテンツ鍵で暗号化された上記コンテンツデータと共に保持している上記コンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とを上記コンテンツデータの利用権を記述する使用許諾条件情報と、上記コンテンツデータの利用分の課金情報とを生成させるために上記他の情報受信装置に引き渡す

ことを特徴とする請求の範囲第 1 8 9 項に記載のコンテンツの利用方法。

1 9 5. 上記コンテンツ鍵を上記他の情報受信装置との間で共有している一時鍵で暗号化する暗号化ステップを具え、

上記引渡ステップは、

上記他の情報受信装置に上記取扱方針データ及び上記価格情報と共に、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記一時鍵で暗号化された上記コンテンツ鍵とを引き渡す

ことを特徴とする請求の範囲第 1 9 4 項に記載のコンテンツの利用方法。

1 9 6. 情報送信装置から配信されるコンテンツデータを受信する情報受信装置のコンテンツの利用方法において、

上記コンテンツデータを利用するための登録情報が異なる他の情報受信装置との間で上記登録情報を授受する授受ステップと、

上記登録情報により上記他の情報受信装置との間で上記コンテンツデータの利用可否を相互に判断する判断ステップと、

上記コンテンツデータの利用権を有しない場合に、上記コンテンツデータの利用可であると判断された上記他の情報受信装置のうち、上記コンテンツデータの利用権を有する情報受信装置から上記利用権を受け取り上記コンテンツデータを利用可能とする受取ステップと

を具えることを特徴とするコンテンツの利用方法。

1 9 7. 上記コンテンツデータの利用分の課金情報を生成して保持する生成保持ステップ

を具えることを特徴とする請求の範囲第 1 9 6 項に記載のコンテンツの利用方法。

198. 上記受取ステップは、

上記コンテンツデータの利用権を有する情報受信装置から送信される、上記コンテンツデータを暗号化している所定のコンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とを受け取り、

上記生成保持ステップは、

上記取扱方針データ及び上記価格情報に基づいて上記課金情報を生成して保持する

ことを特徴とする請求の範囲第197項に記載のコンテンツの利用方法。

199. 上記取扱方針データ及び上記価格情報に基づいて上記コンテンツデータの利用権を記述した使用許諾条件情報を生成して保持する情報生成ステップ

を具えることを特徴とする請求の範囲第198項に記載のコンテンツの利用方法。

200. 上記受取ステップは、

上記コンテンツデータの利用権を有する情報受信装置から送信される、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記他の情報受信装置との間で共有している一時鍵で暗号化された上記コンテンツ鍵とを受信し、

上記コンテンツ鍵を上記一時鍵で復号し、当該復号した上記コンテンツ鍵を自己固有の保存鍵で暗号化して保存すると共に、上記コンテンツ鍵で暗号化された上記コンテンツデータを保持するコンテンツ保持ステップ

を具えることを特徴とする請求の範囲第187項に記載のコンテンツの利用方法。

201. 情報送信装置から配信されるコンテンツデータを受信する情報受信装置に用いられるプログラム格納媒体において、

上記コンテンツデータを利用するための登録情報が異なる他の情報受信装置と

の間で上記登録情報を授受する授受ステップと、

上記登録情報により上記他の情報受信装置との間で上記コンテンツデータの利用可否を相互に判断する判断ステップと、

上記コンテンツデータの利用権を有する場合に、上記コンテンツデータの利用可であると判断された上記他の情報受信装置に対して上記利用権を引き渡すことにより、上記利用権が引き渡された上記他の情報受信装置で上記コンテンツデータを利用可能とする引渡ステップと

を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

202. 上記コンテンツデータの利用権を引き渡した上記他の情報受信装置で利用する上記コンテンツデータの利用分の課金情報を生成して保持する生成保持ステップ

を具えることを特徴とする請求の範囲第201項に記載のプログラム格納媒体。

203. 上記生成保持ステップは、

所定のコンテンツ鍵で暗号化された上記コンテンツデータと共に保持している上記コンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とに基づいて上記課金情報を生成して保持する

ことを特徴とする請求の範囲第202項に記載のプログラム格納媒体。

204. 上記取扱方針データ及び上記価格情報に基づいて上記コンテンツデータの利用権を記述した使用許諾条件情報を生成する生成ステップを具え、

上記引渡ステップは、

上記他の情報受信装置に上記コンテンツデータの利用権として、上記使用許諾条件情報を引き渡す

ことを特徴とする請求の範囲第 2 0 3 項に記載のプログラム格納媒体。

2 0 5. 上記コンテンツ鍵を上記他の情報受信装置との間で共有している一時鍵で暗号化する暗号化ステップを具え、

上記引渡ステップは、

上記他の情報受信装置に上記使用許諾条件情報と共に、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記一時鍵で暗号化された上記コンテンツ鍵とを送信する

ことを特徴とする請求の範囲第 2 0 4 項に記載のプログラム格納媒体。

2 0 6. 上記引渡ステップは、

所定のコンテンツ鍵で暗号化された上記コンテンツデータと共に保持している上記コンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とを上記コンテンツデータの利用権を記述する使用許諾条件情報と、上記コンテンツデータの利用分の課金情報とを生成させるために上記他の情報受信装置に引き渡す

ことを特徴とする請求の範囲第 2 0 1 項に記載のプログラム格納媒体。

2 0 7. 上記コンテンツ鍵を上記他の情報受信装置との間で共有している一時鍵で暗号化する暗号化ステップを具え、

上記引渡ステップは、

上記他の情報受信装置に上記取扱方針データ及び上記価格情報と共に、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記一時鍵で暗号化された上記コンテンツ鍵とを引き渡す

ことを特徴とする請求の範囲第 2 0 6 項に記載のプログラム格納媒体。

2 0 8. 情報送信装置から配信されるコンテンツデータを受信する情報受信装置

に用いられるプログラム格納媒体において、

上記コンテンツデータを利用するための登録情報が異なる他の情報受信装置との間で上記登録情報を授受する授受ステップと、

上記登録情報により上記他の情報受信装置との間で上記コンテンツデータの利用可否を相互に判断する判断ステップと、

上記コンテンツデータの利用権を有しない場合に、上記コンテンツデータの利用可であると判断された上記他の情報受信装置のうち、上記コンテンツデータの利用権を有する情報受信装置から上記利用権を受け取り上記コンテンツデータを利用可能とする受取ステップと

を具えることを特徴とするプログラムを情報受信装置に実行させるプログラム格納媒体。

209. 上記コンテンツデータの利用分の課金情報を生成して保持する生成保持ステップ

を具えることを特徴とする請求の範囲第208項に記載のプログラム格納媒体。

210. 上記受取ステップは、

上記コンテンツデータの利用権を有する情報受信装置から送信される、上記コンテンツデータを暗号化している所定のコンテンツ鍵の取扱方針を記述した取扱方針データと、上記コンテンツデータの価格情報とを受け取り、

上記生成保持ステップは、

上記取扱方針データ及び上記価格情報に基づいて上記課金情報を生成して保持する

ことを特徴とする請求の範囲第209項に記載のプログラム格納媒体。

211. 上記取扱方針データ及び上記価格情報に基づいて上記コンテンツデータ

の利用権を記述した使用許諾条件情報を生成して保持する情報生成ステップ  
を具えることを特徴とする請求の範囲第 2 1 0 項に記載のプログラム格納媒体  
。

2 1 2. 上記受取ステップは、

上記コンテンツデータの利用権を有する情報受信装置から送信される、上記コンテンツ鍵で暗号化された上記コンテンツデータと、上記他の情報受信装置との間で共有している一時鍵で暗号化された上記コンテンツ鍵とを受信し、

上記コンテンツ鍵を上記一時鍵で復号し、当該復号した上記コンテンツ鍵を自己固有の保存鍵で暗号化して保存すると共に、上記コンテンツ鍵で暗号化された上記コンテンツデータを保持するコンテンツ保持ステップ

を具えることを特徴とする請求の範囲第 2 1 1 項に記載のプログラム格納媒体  
。



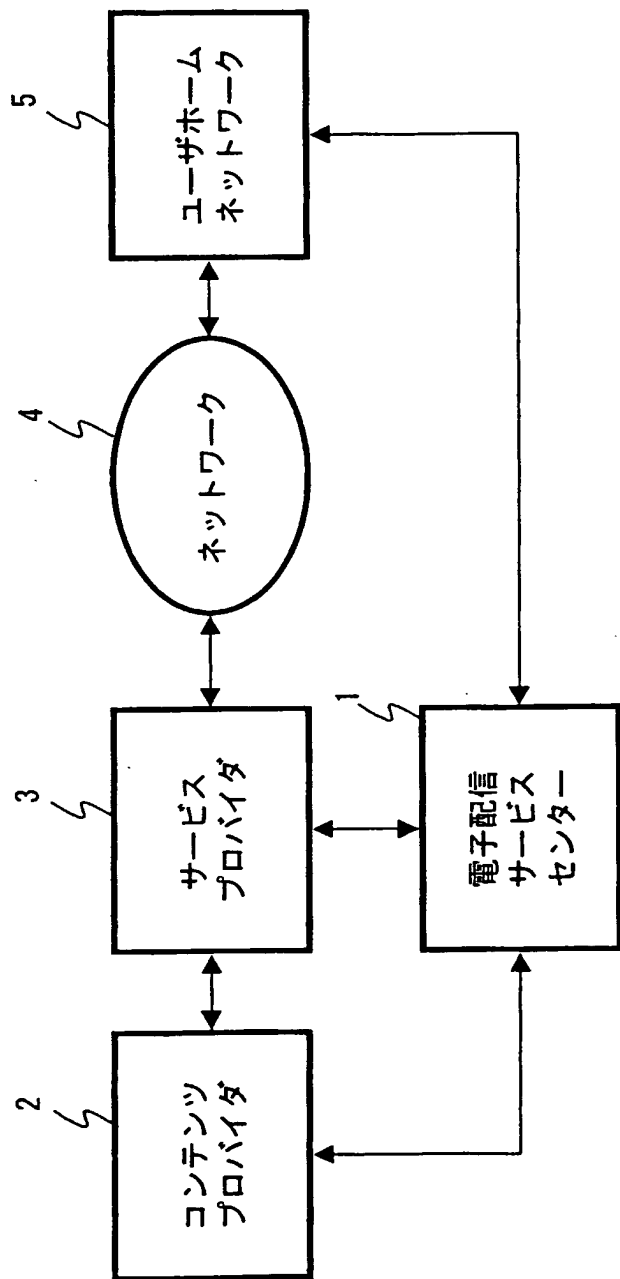


図 1

**This Page Blank (uspto)**

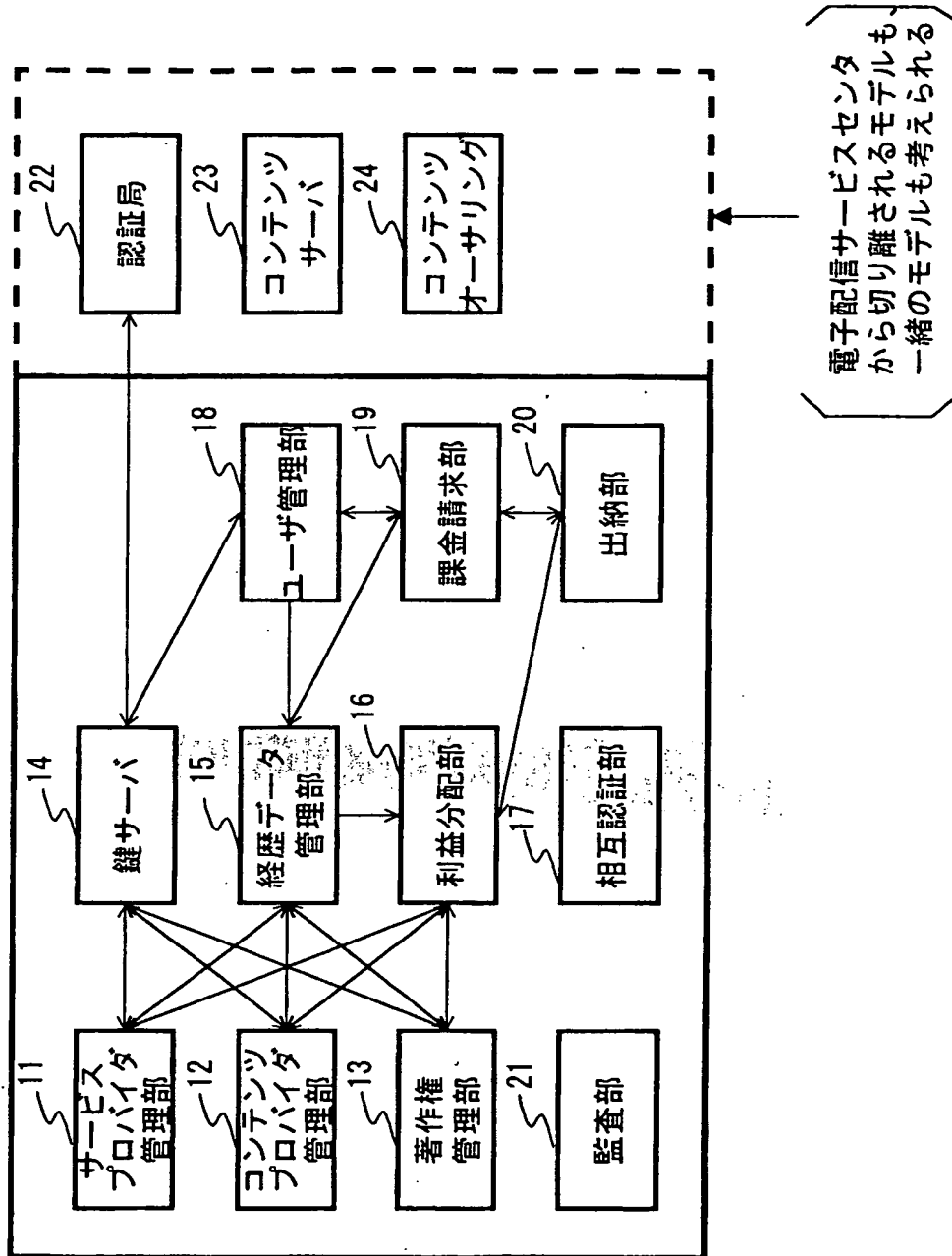


図 2

**This Page Blank (uspto)**

電子配信サービスセンタが有する配信用・個別鍵

配信鍵	個別鍵	バージョン	使用可能期間 開始	終了
aaaaaaaa	zzzzzzzz	1	2000/1/1	2000/1/31
bbbbbbbb	vvvvvvvv	2	2000/2/1	2000/2/29
cccccccc	xxxxxxx	3	2000/3/1	2000/3/31
dddddddd	wwwwwww	4	2000/4/1	2000/4/30
eeeeeeee	vvvvvvvv	5	2000/5/1	2000/5/31
ffffffff	uuuuuuuu	6	2000/6/1	2000/6/30

使用する  
鍵

個別鍵  
を送信

を配  
送鍵  
送信

ホームサーバが有する配信鍵

配信鍵	バージョン	使用可能期間 開始	終了
aaaaaaaa	1	2000/1/1	2000/1/31
bbbbbbbb	2	2000/2/1	2000/2/29
cccccccc	3	2000/3/1	2000/3/31

使用する  
配信鍵

コンテンツプロバイダが有する個別鍵

個別鍵	バージョン	使用可能期間 開始	終了
zzzzzzzz	1	2000/1/1	2000/1/31
vvvvvvvv	2	2000/2/1	2000/2/29
xxxxxxx	3	2000/3/1	2000/3/31
wwwwwww	4	2000/4/1	2000/4/30
vvvvvvvv	5	2000/5/1	2000/5/31
uuuuuuuu	6	2000/6/1	2000/6/30

使用する  
個別鍵

図 3

**This Page Blank (uspto)**

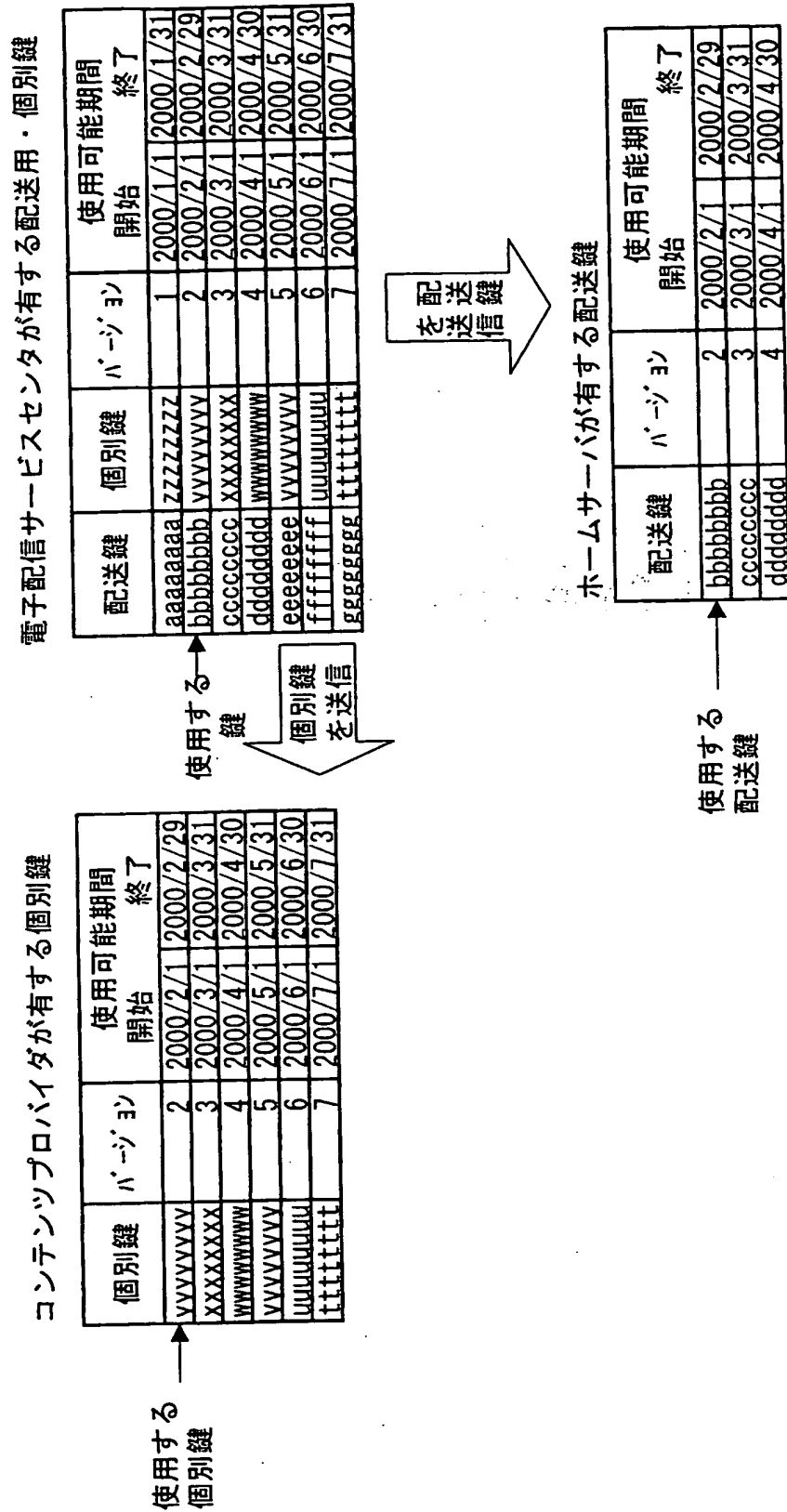


図 4

**This Page Blank (uspto)**



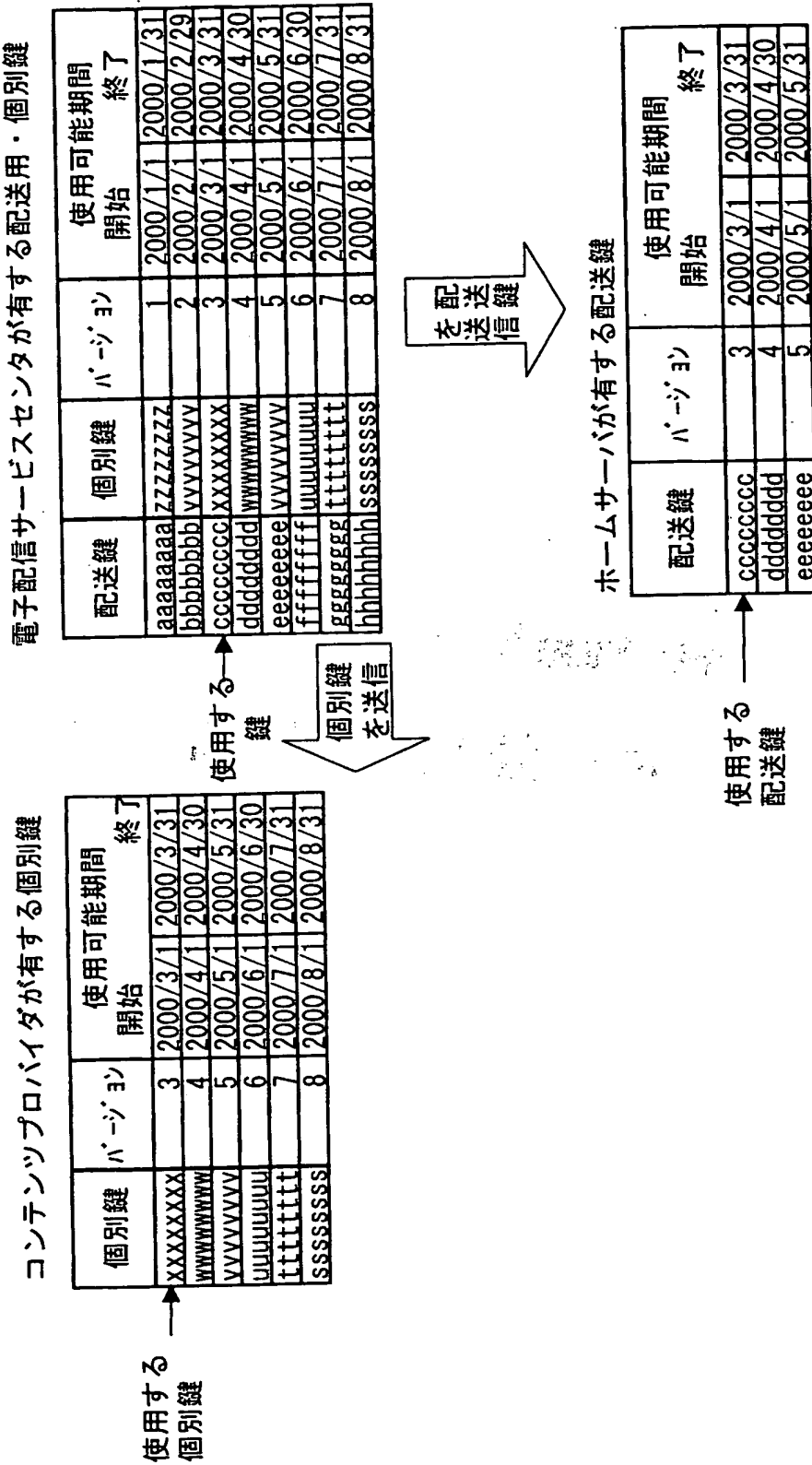


図 5

**This Page Blank (uspto)**

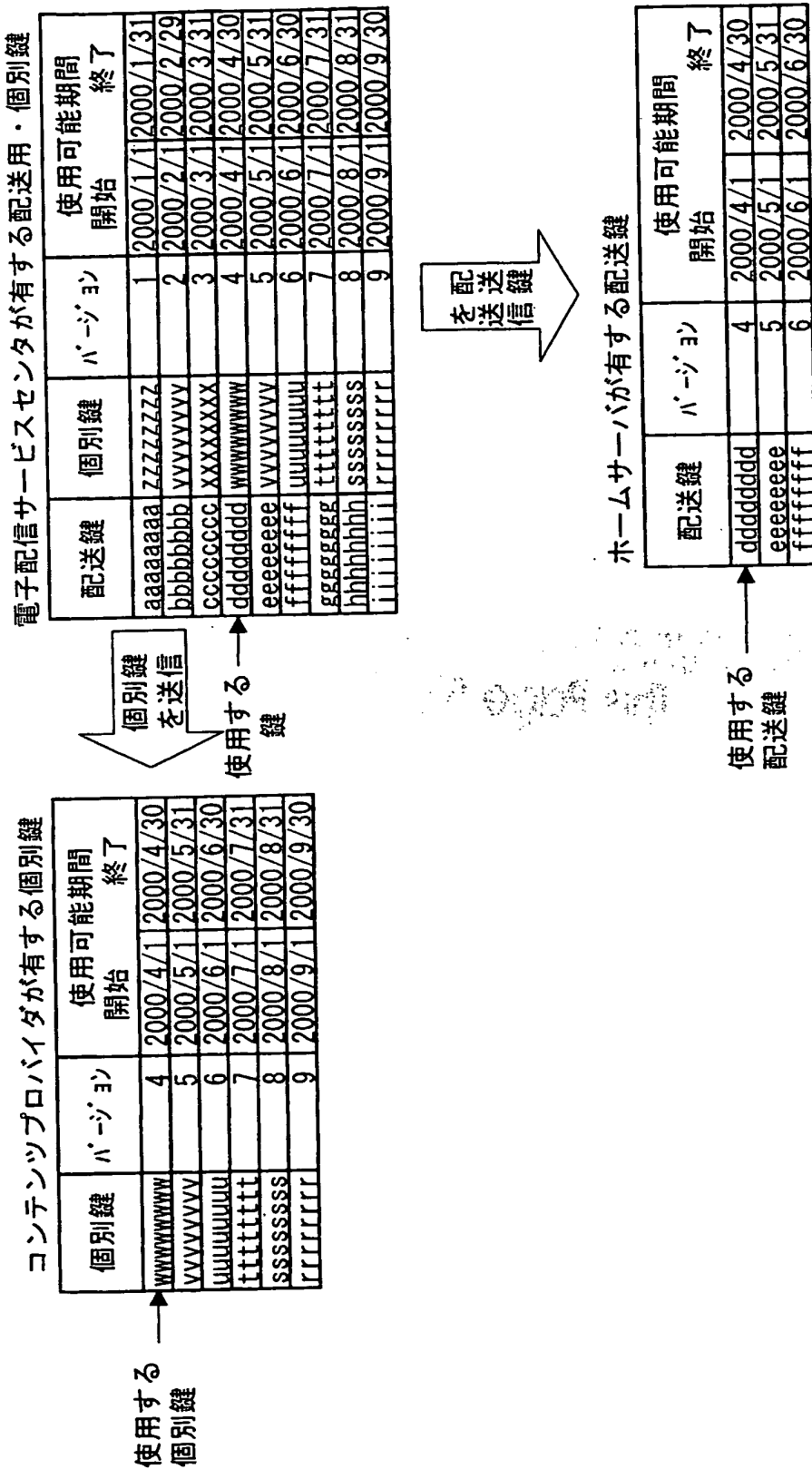


図 6

**THIS PAGE BLANK (USPTO)**

グループID	ID	サービスセンタとの接続	決済処理	購入処理	代理決済者	代理購入者	登録
GpID1	ID1	可	可	可	—	—	可
	ID2	可	不可	可	ID1	—	可
	ID3	可	不可	可	ID1	—	不可
	ID4	不可	不可	不可	—	ID1	可
	ID5	不可	不可	不可	—	ID2	不可
GpID2	ID6	可	可	可	—	—	不可
	ID7	可	不可	可	ID6	—	不可
	ID8	可	不可	可	ID6	—	可
	ID9	不可	不可	不可	—	ID6.7.8	不可
	ID10	不可	不可	不可	—	ID6.7.8	可
GpID3	ID11	可	可	可	—	—	不可
	ID12	可	不可	可	ID11	—	不可
	ID13	可	不可	可	ID11	—	可
	ID14	不可	不可	不可	—	ID11.12.13	不可
	ID15	不可	不可	不可	—	ID11	可
. . .							

図 7

**THIS PAGE BLANK (USPTO)**

グループID	ID	サービスセットとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
Gp1D1	ID1	可	可	決済ID1	可	—	—	可	署名
	ID2	可	不可	—	可	ID1	—	可	
	ID3	可	不可	—	可	ID1	—	不可	
	ID4	不可	不可	—	不可	—	ID1	可	
	ID5	不可	不可	—	不可	—	ID2	不可	

(A)

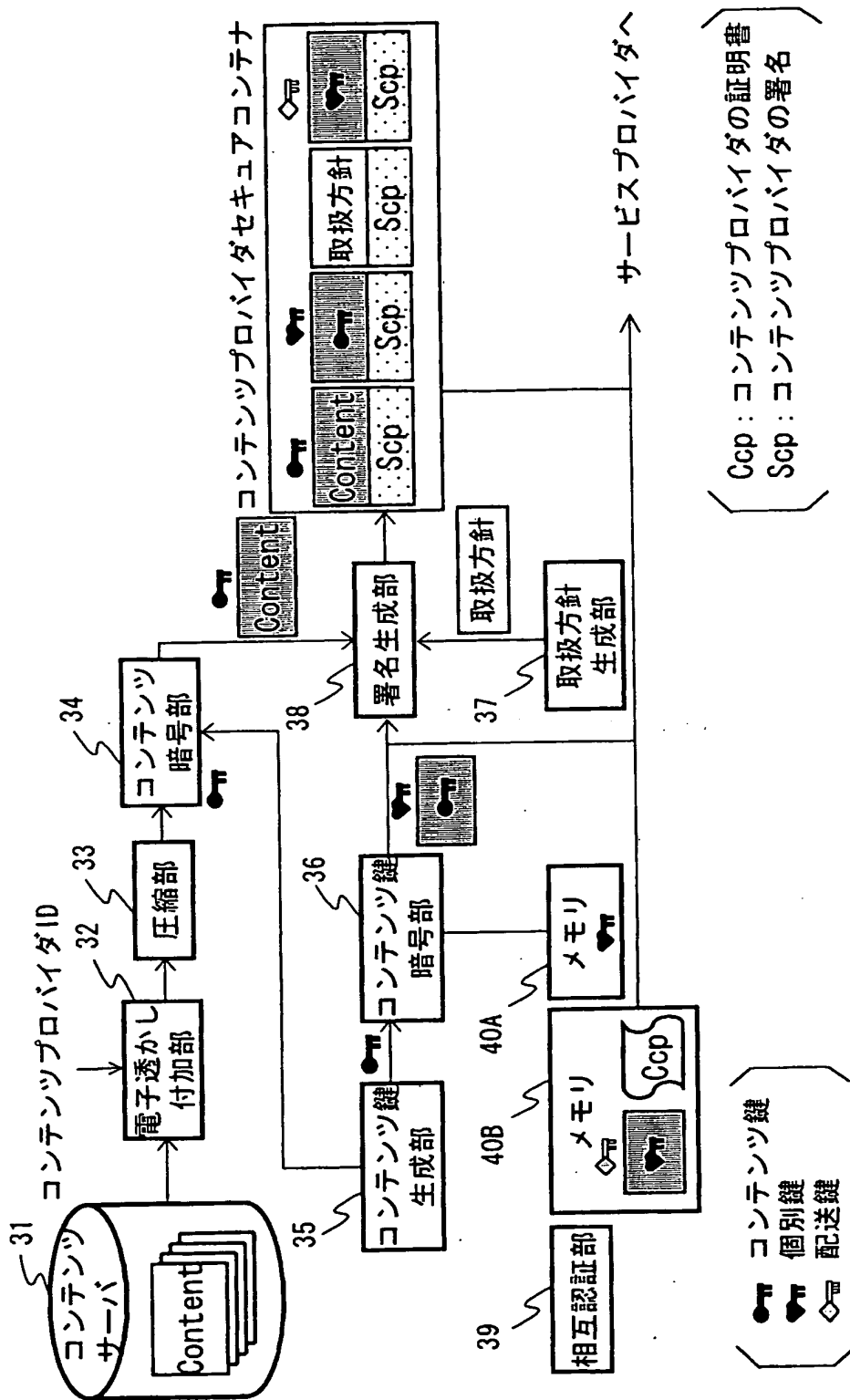
グループID	ID	サービスセットとの接続	決済処理	決済ID	購入処理	代理決済者	代理購入者	登録	署名
Gp1D2	ID6	可	可	決済ID2	可	—	—	可	署名
	ID7	可	不可	—	可	ID6	—	可	
	ID8	可	不可	—	可	ID6	—	不可	
	ID9	不可	不可	—	不可	—	ID6.7.8	可	
	ID10	不可	不可	—	不可	—	ID6.7.8	不可	

(B)

図 8

**THIS PAGE BLANK (USPTO)**





9  
✕

**THIS PAGE BLANK (USPTO)**

## (署名生成)

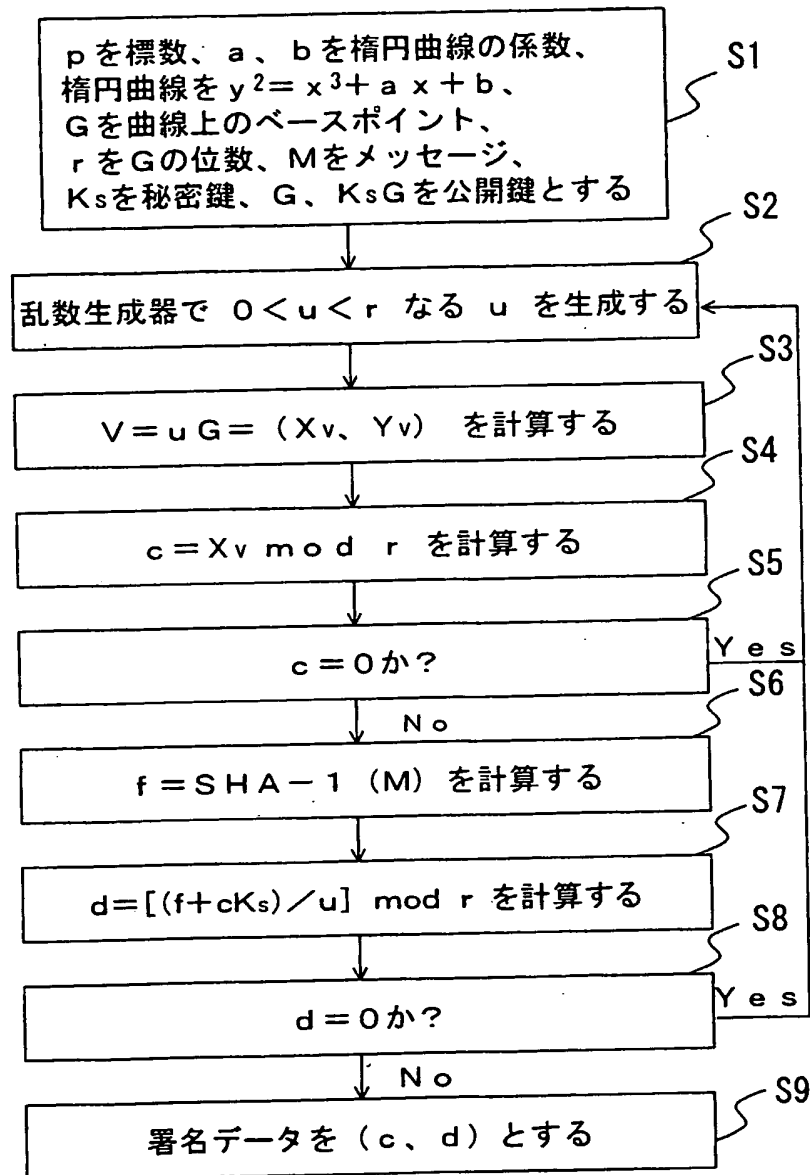


図10

**THIS PAGE BLANK (USPTO)**

## (署名検証)

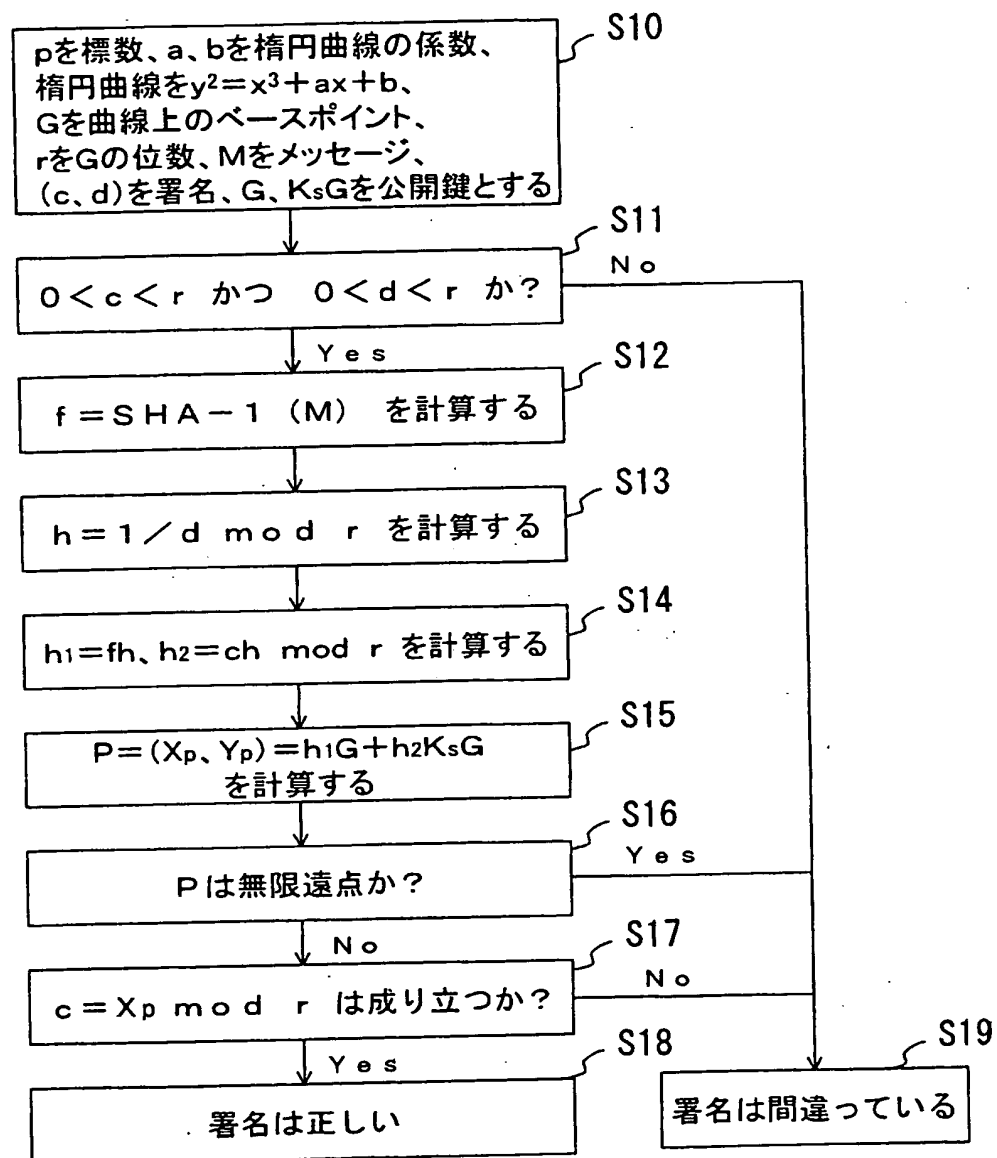


図 1 1

**THIS PAGE BLANK (USPTO)**

## (暗号化)

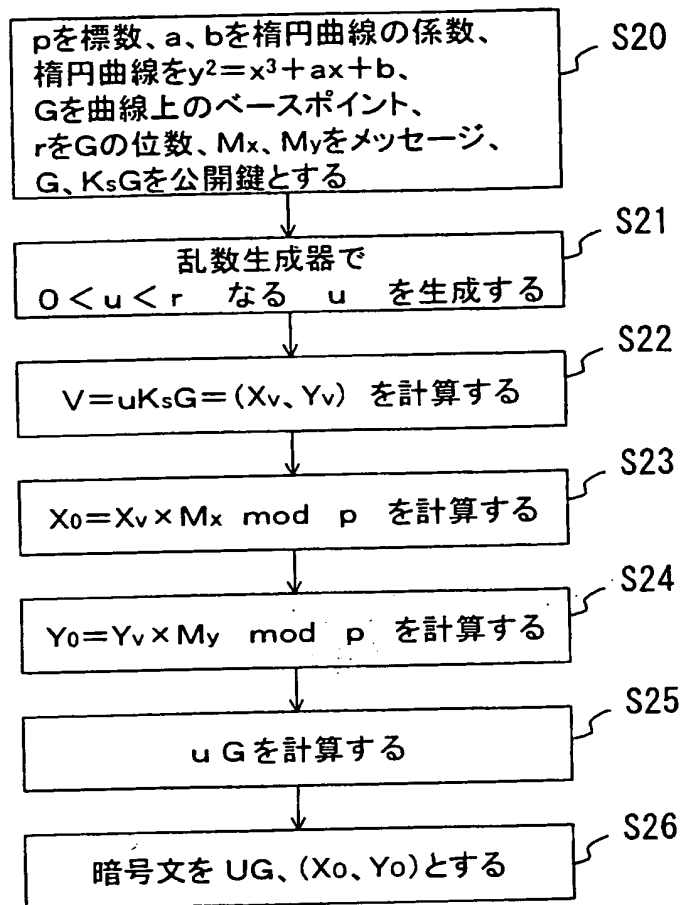


図 1 2

**THIS PAGE BLANK (USPTO)**



## (復号化)

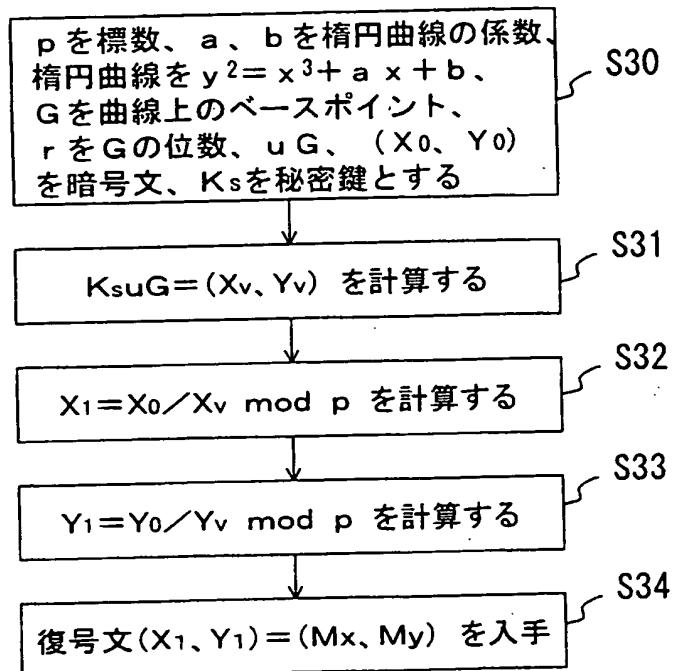
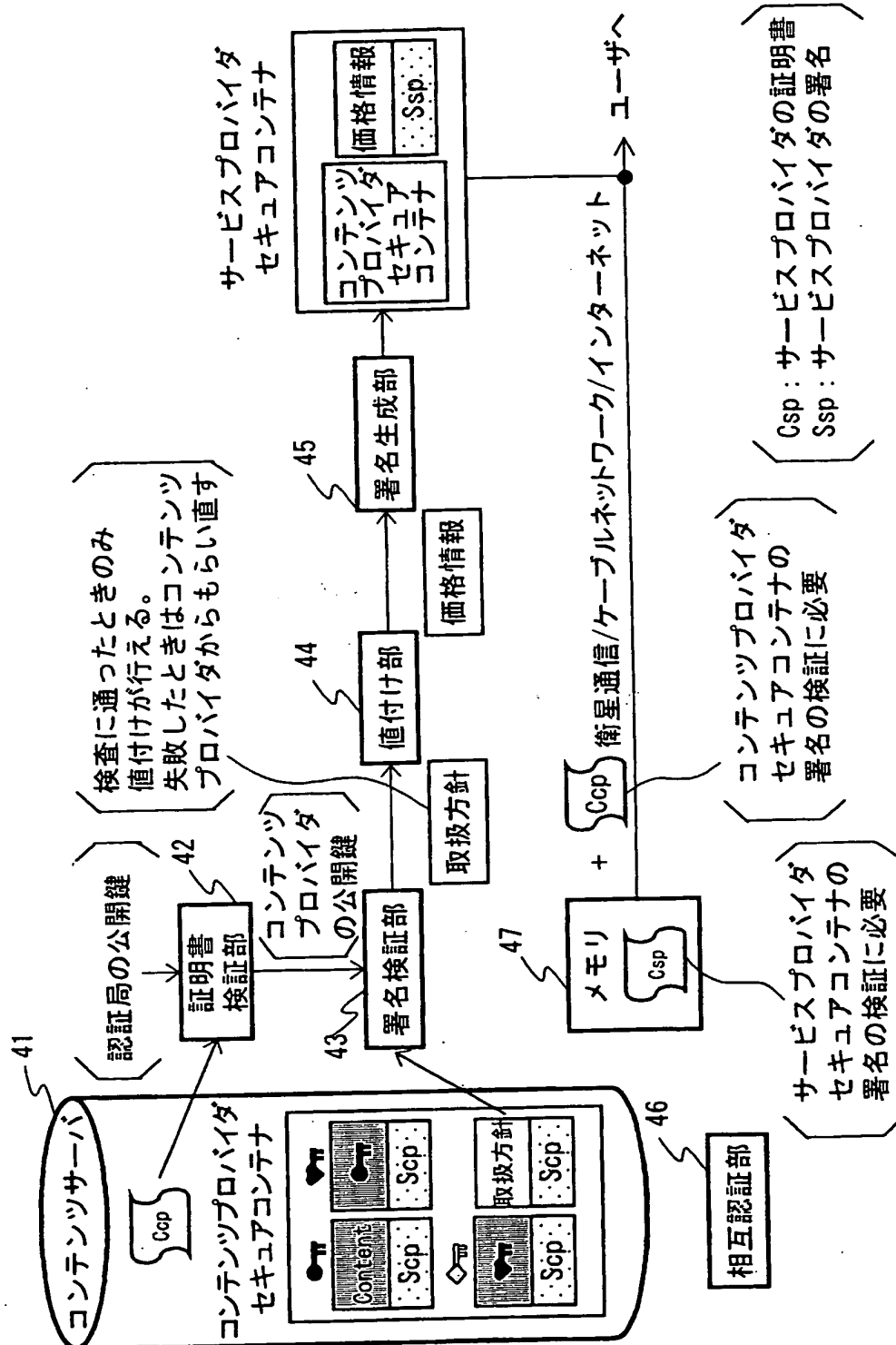


図 1 3

**THIS PAGE BLANK (USPTO)**



41X

**THIS PAGE BLANK (USPTO)**

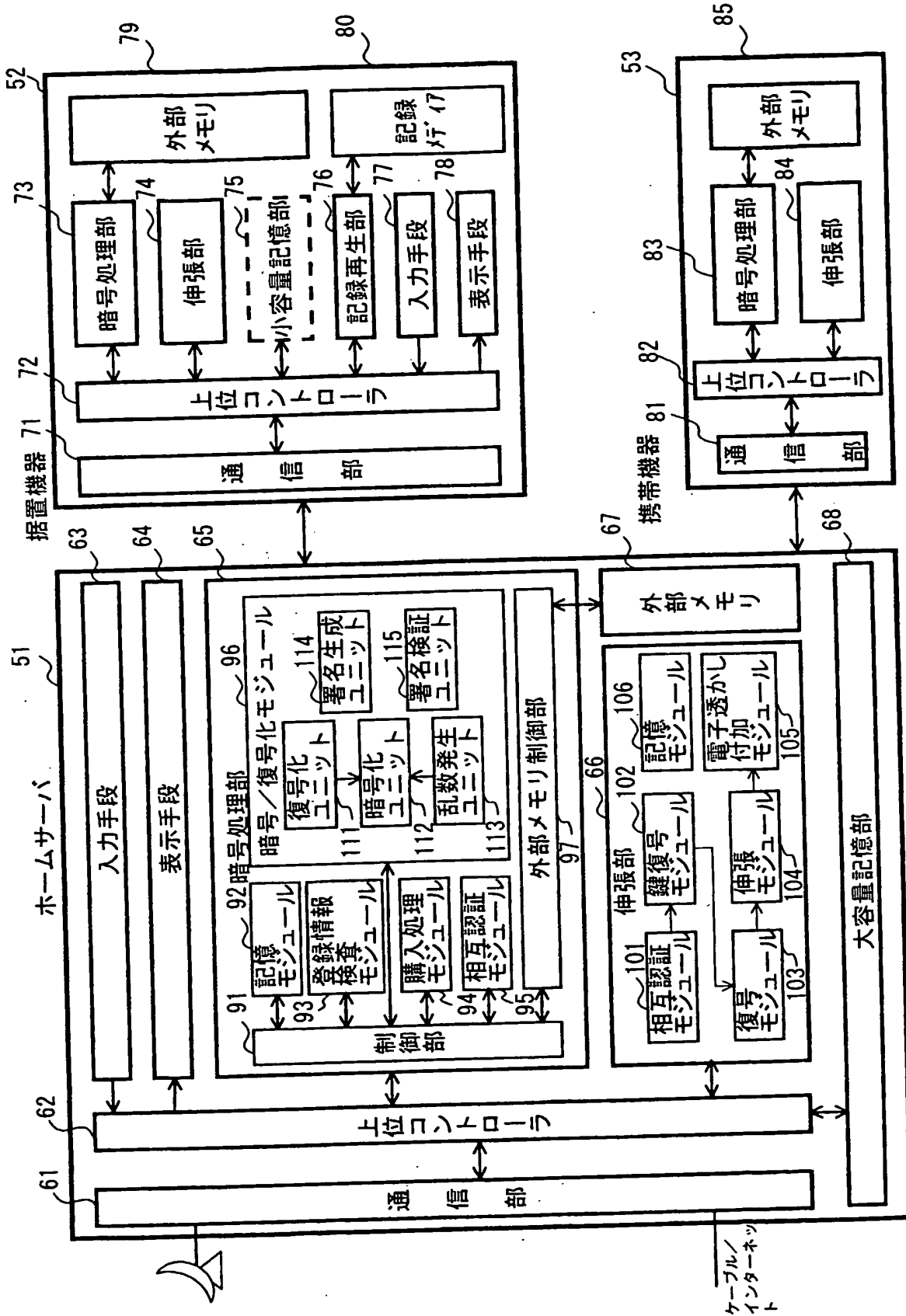


図15

**THIS PAGE BLANK (USPTO)**

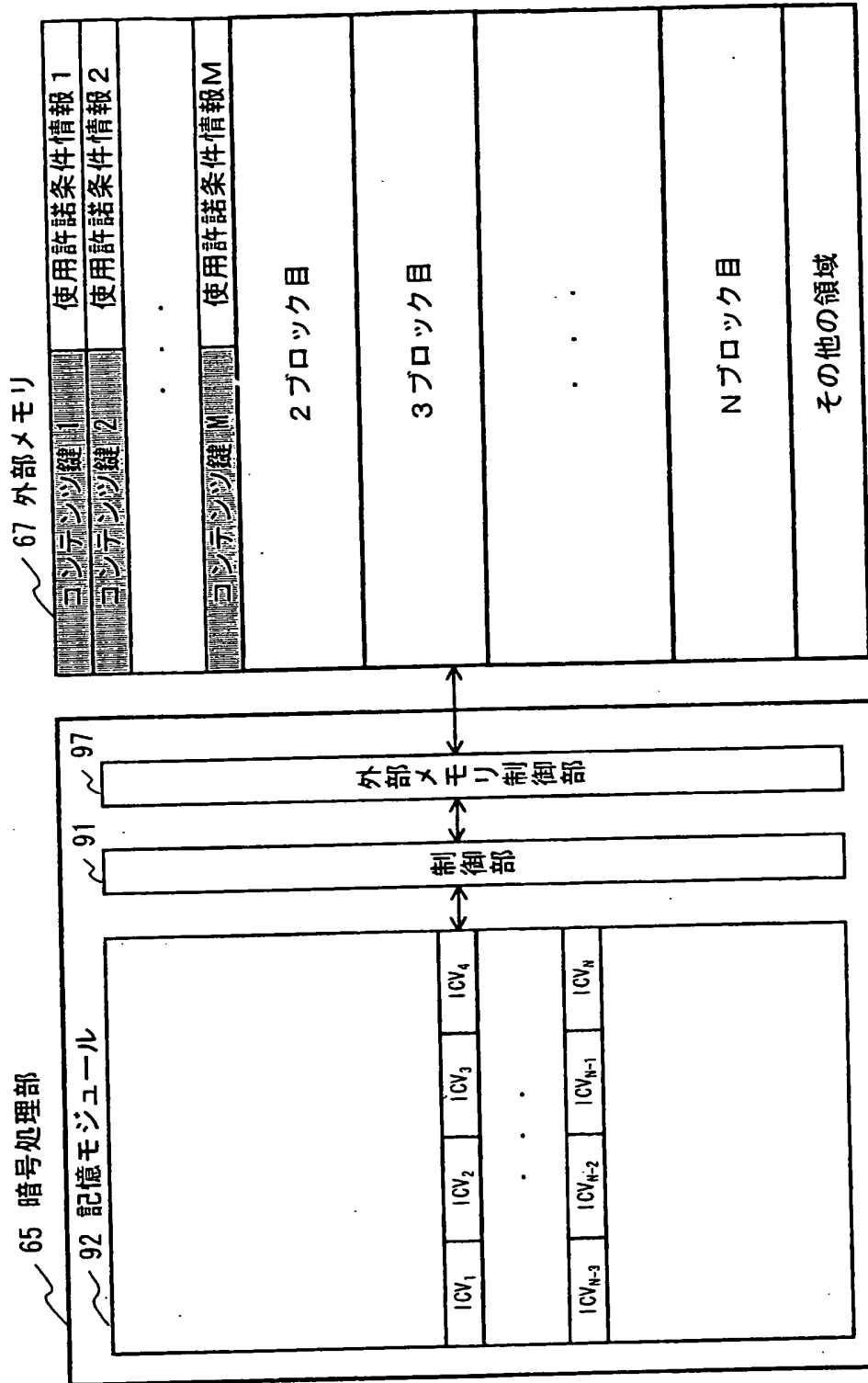


図16

**THIS PAGE BLANK (USPTO)**



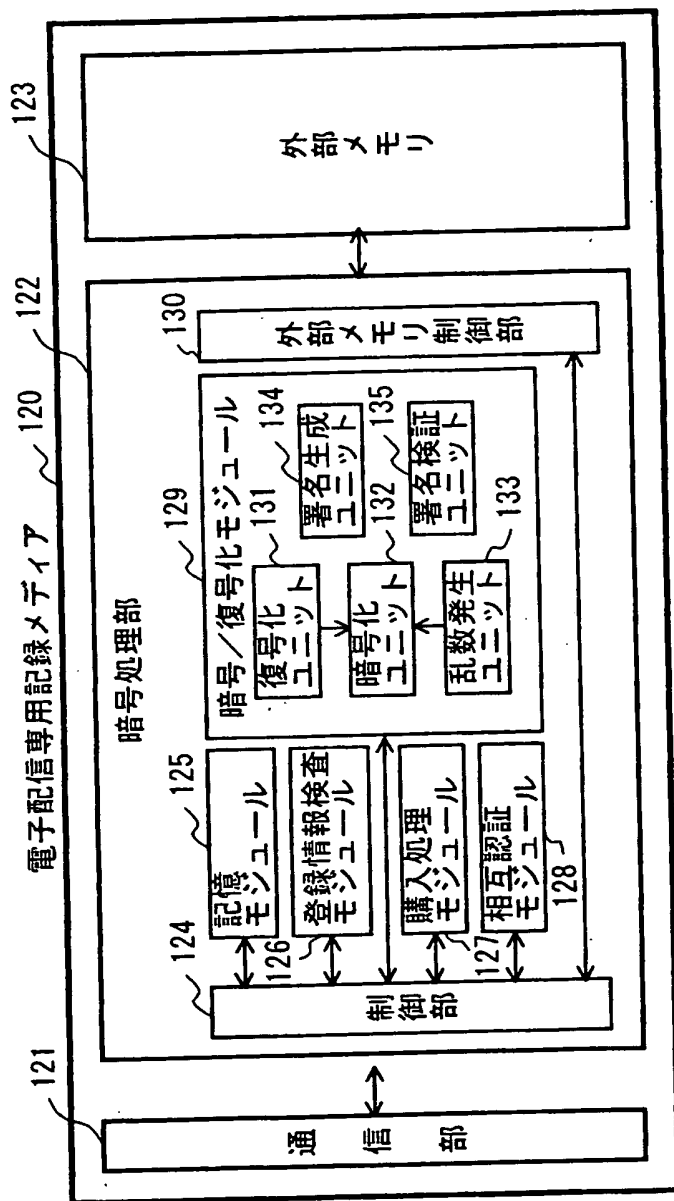


図17

**THIS PAGE BLANK (USPTO)**

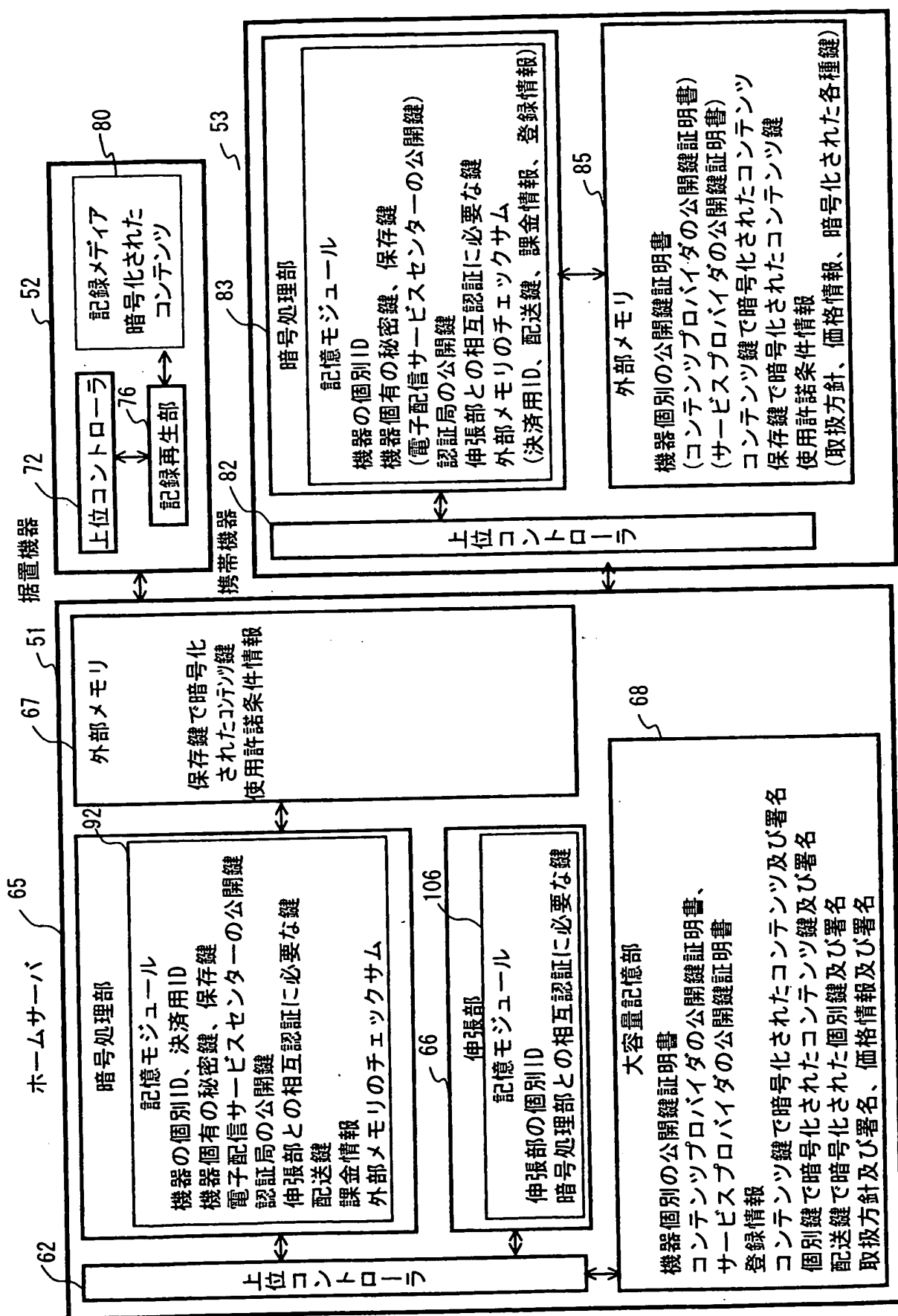


図 18

**THIS PAGE BLANK (USPTO)**

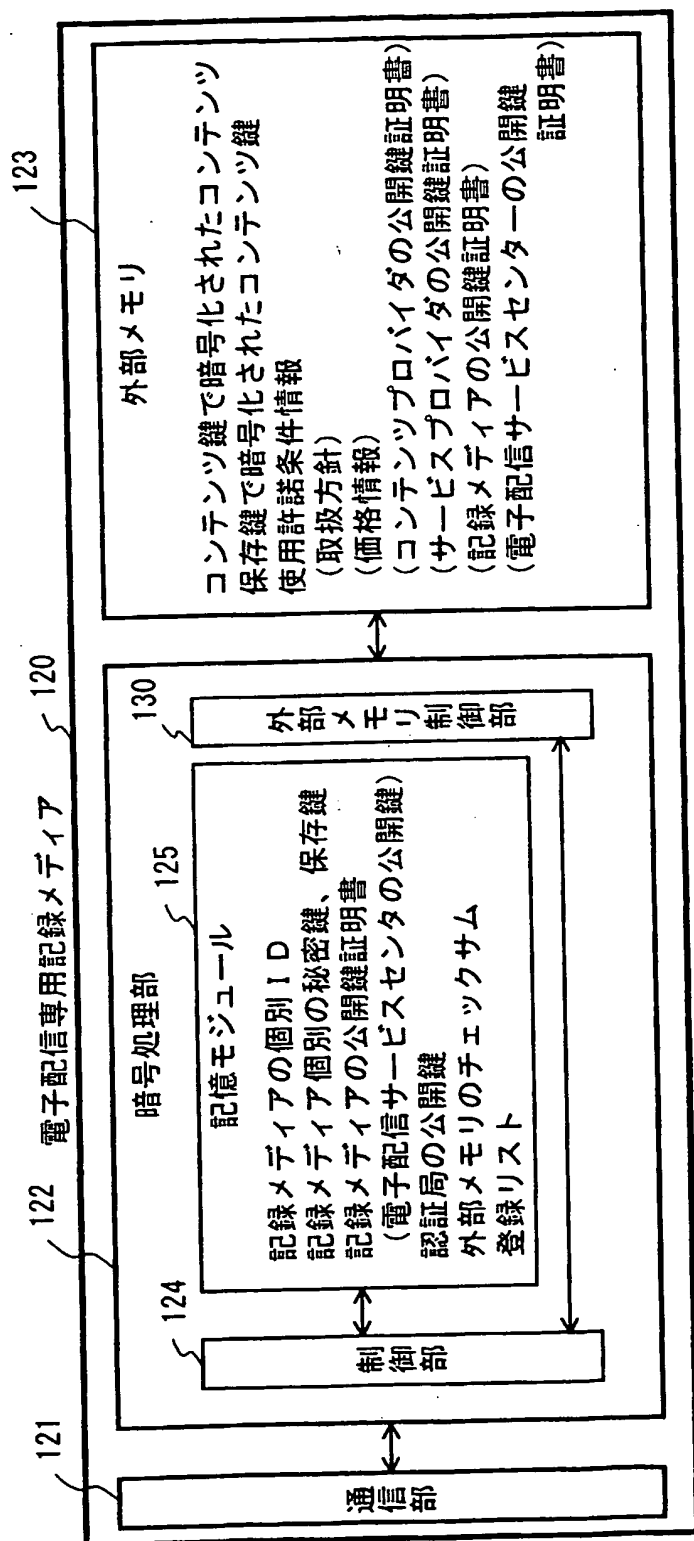


図19

**THIS PAGE BLANK (USPTO)**

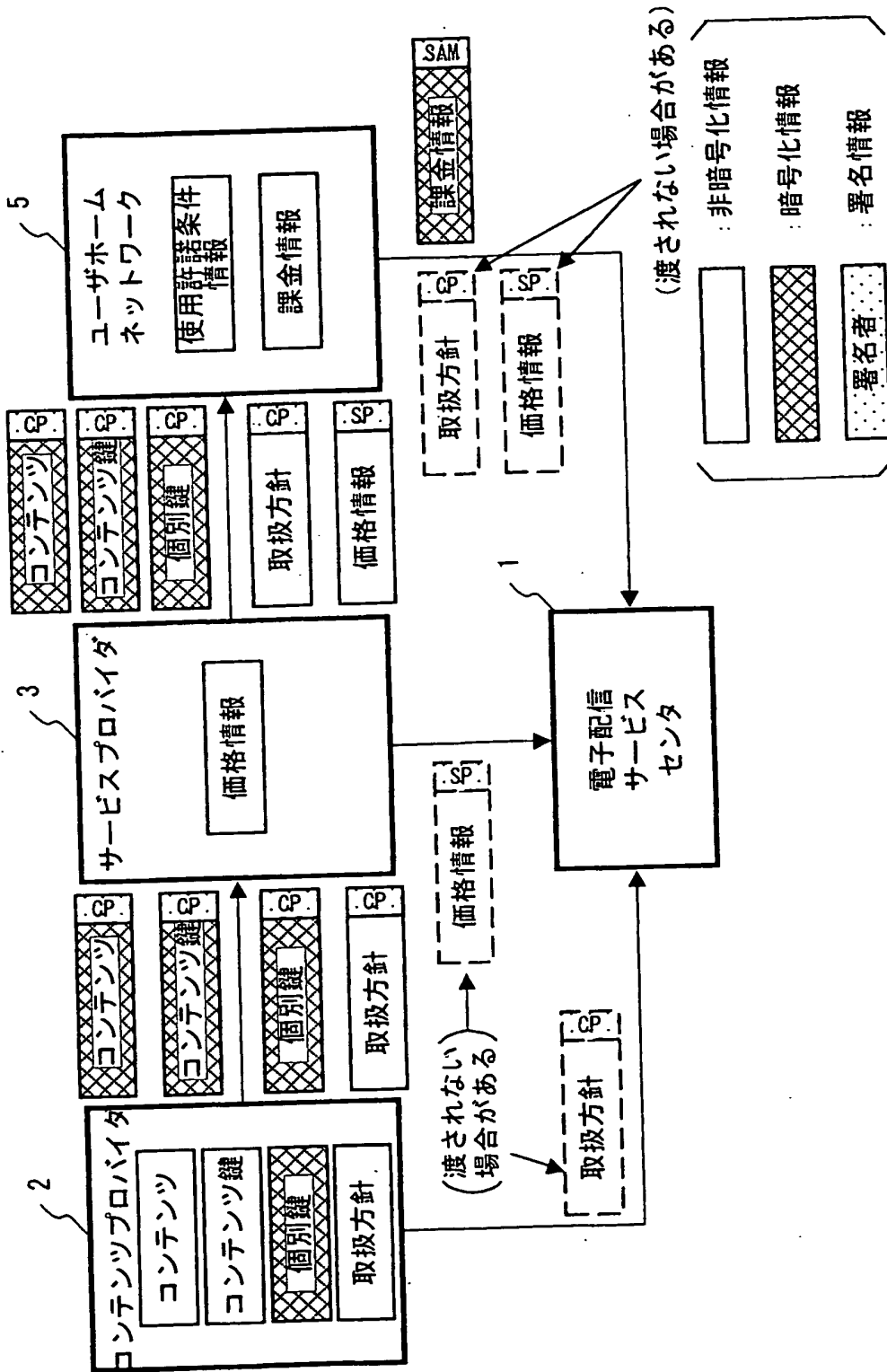


図20

**THIS PAGE BLANK (USPTO)**



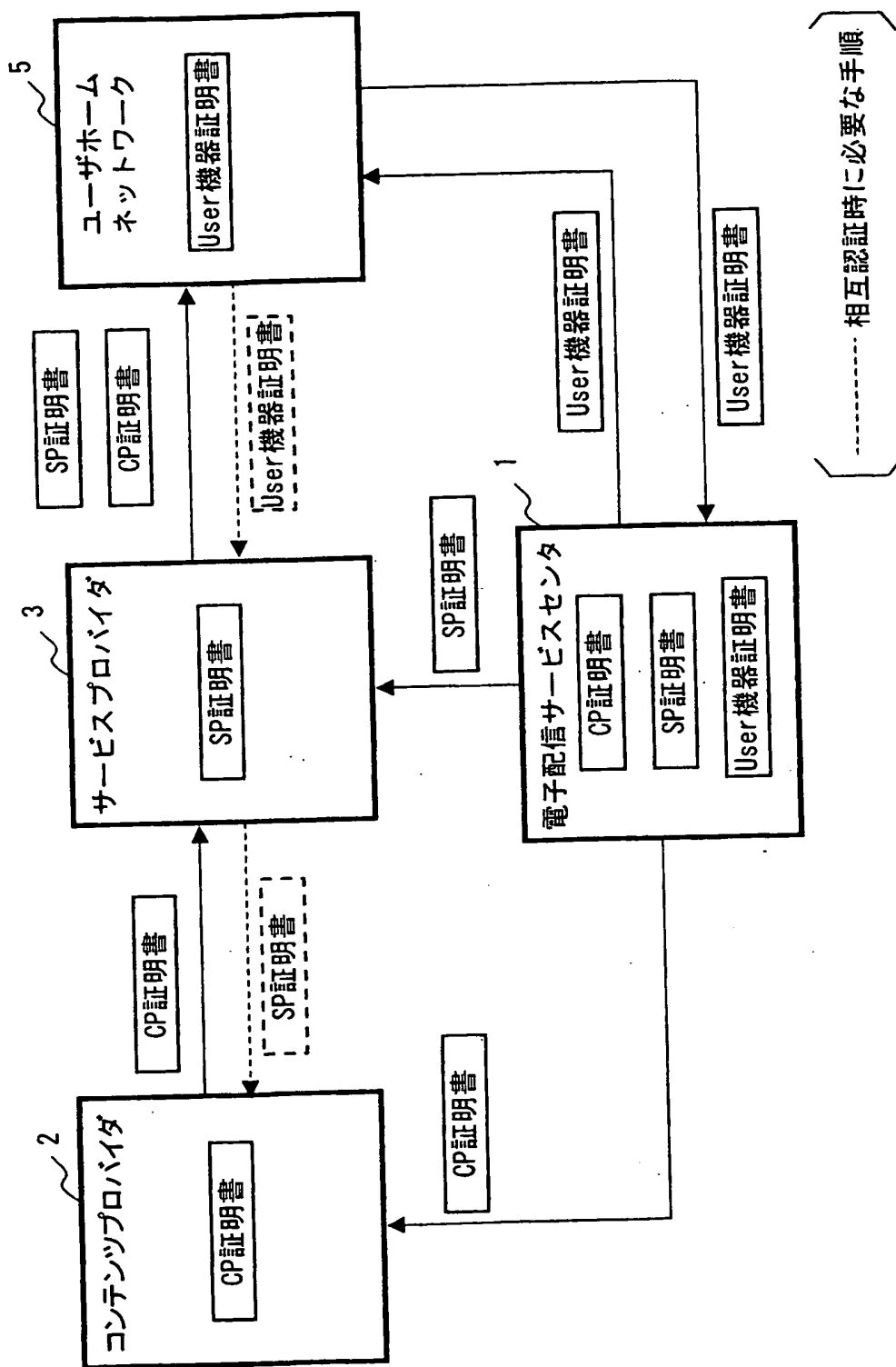


図 2 1

**THIS PAGE BLANK (USPTO)**

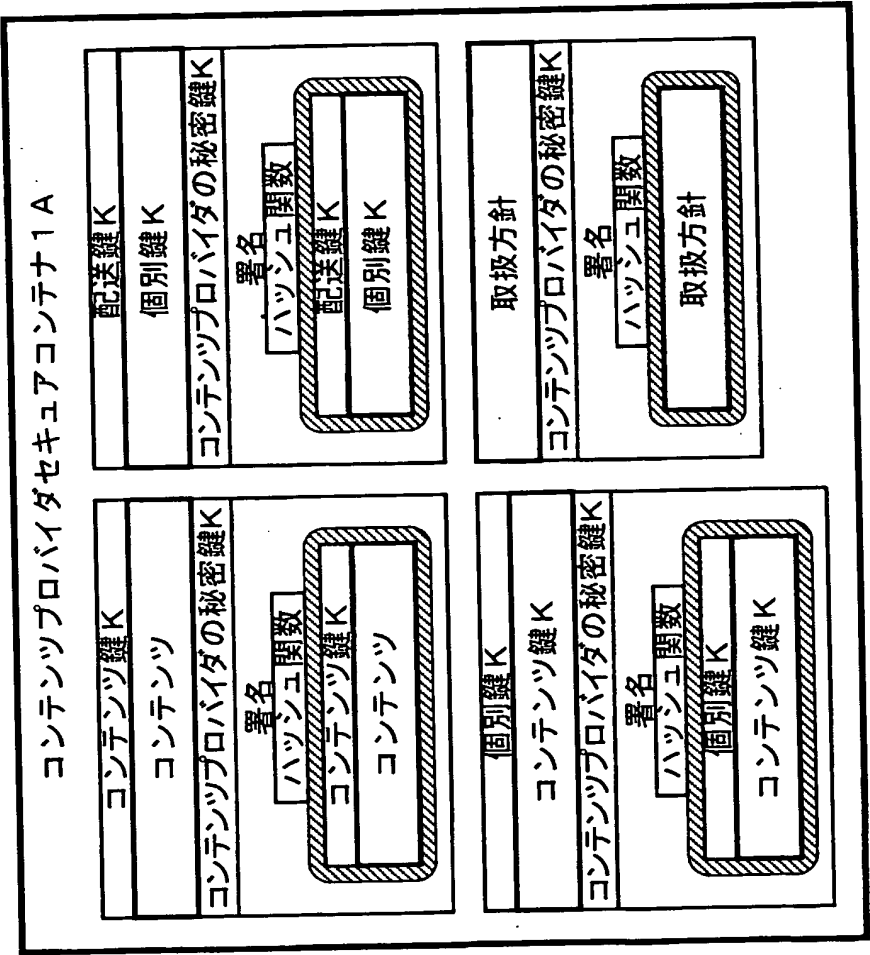


図 2 2

**THIS PAGE BLANK (USPTO)**

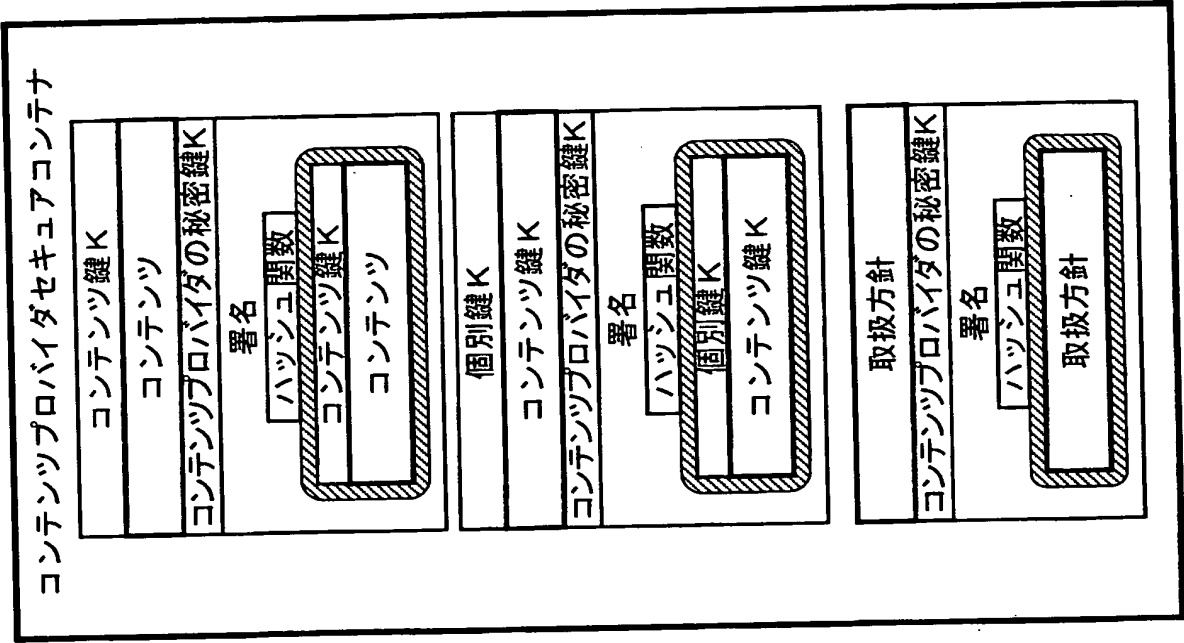


図 23

**THIS PAGE BLANK (USPTO)**

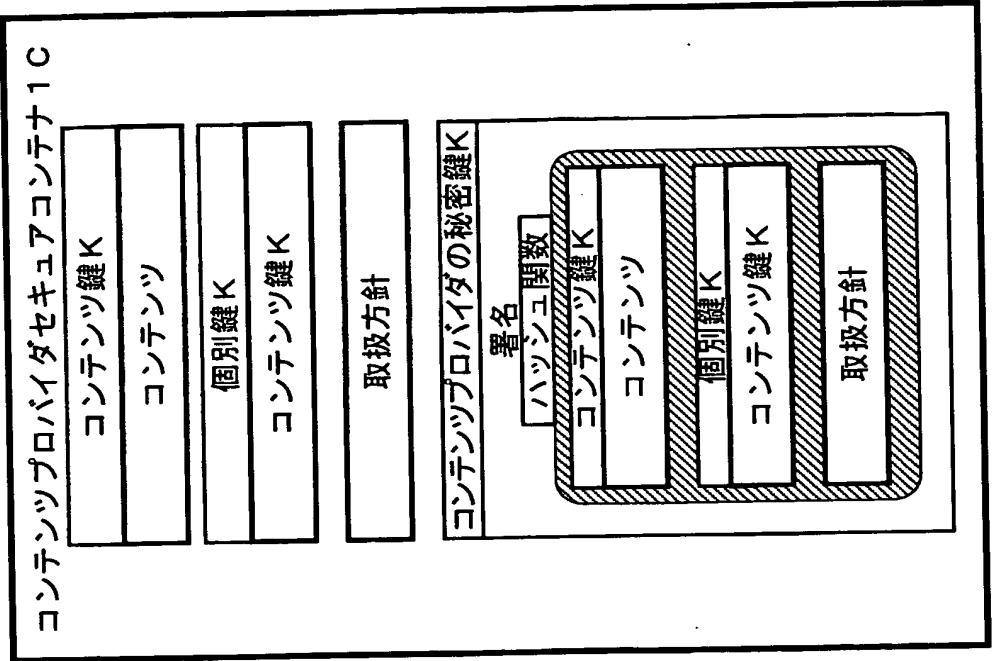


図 2 4

**THIS PAGE BLANK (USPTO)**



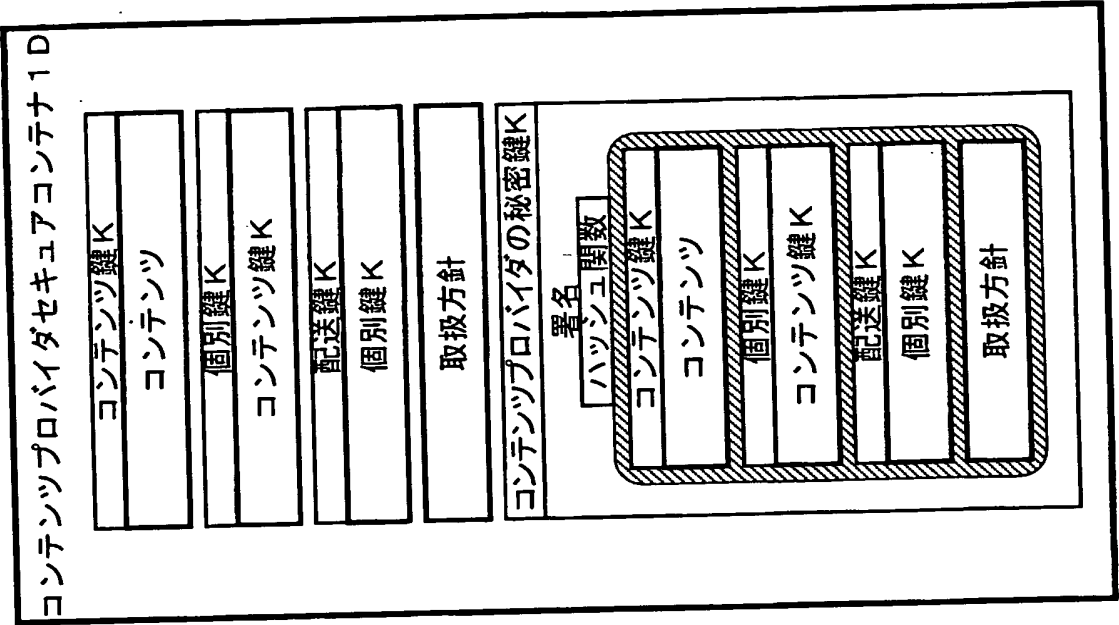


図 2 5

**THIS PAGE BLANK (USPTO)**

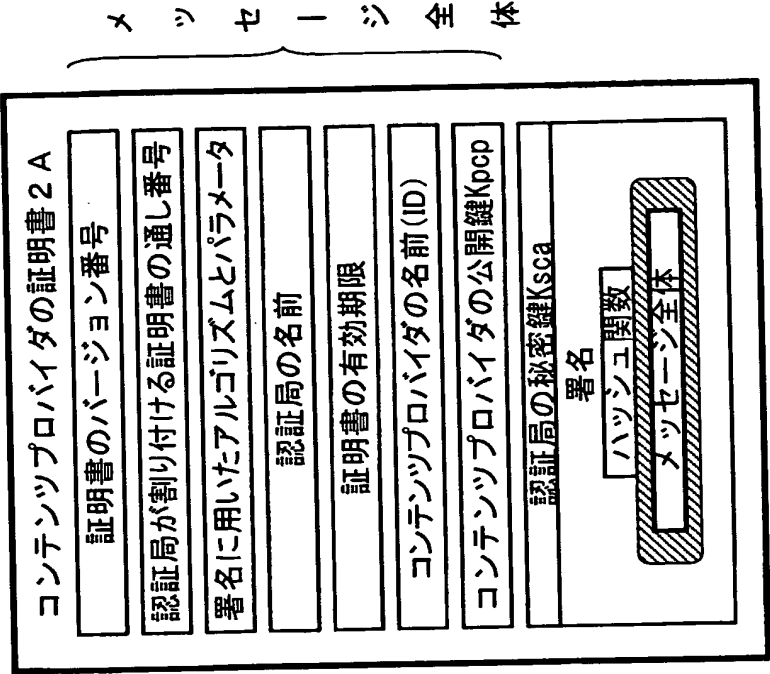


図 2 6

**THIS PAGE BLANK (USPTO)**

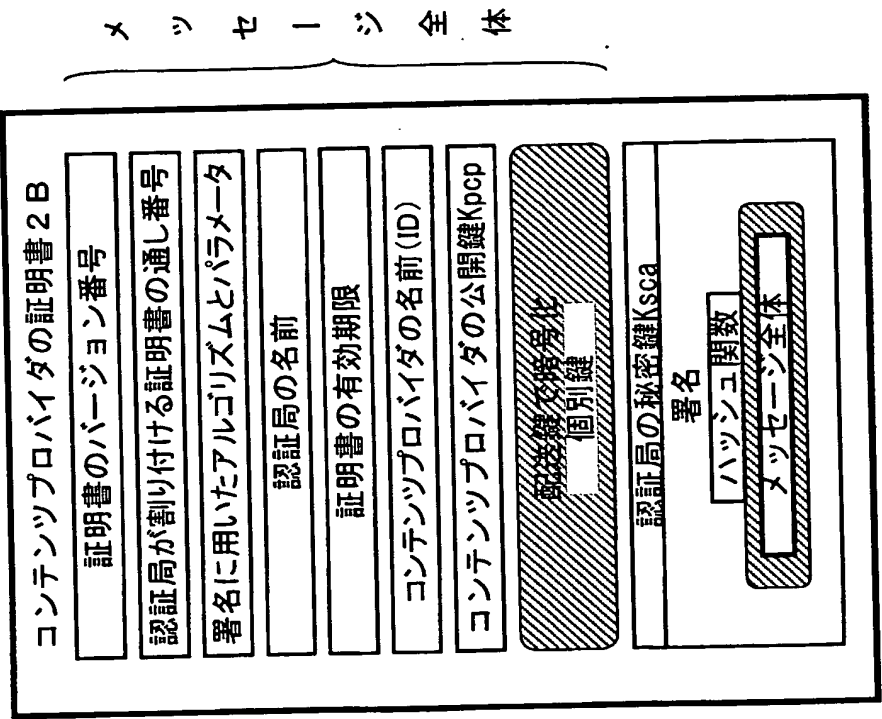


図 27

**THIS PAGE BLANK (USPTO)**

メッセージ全体

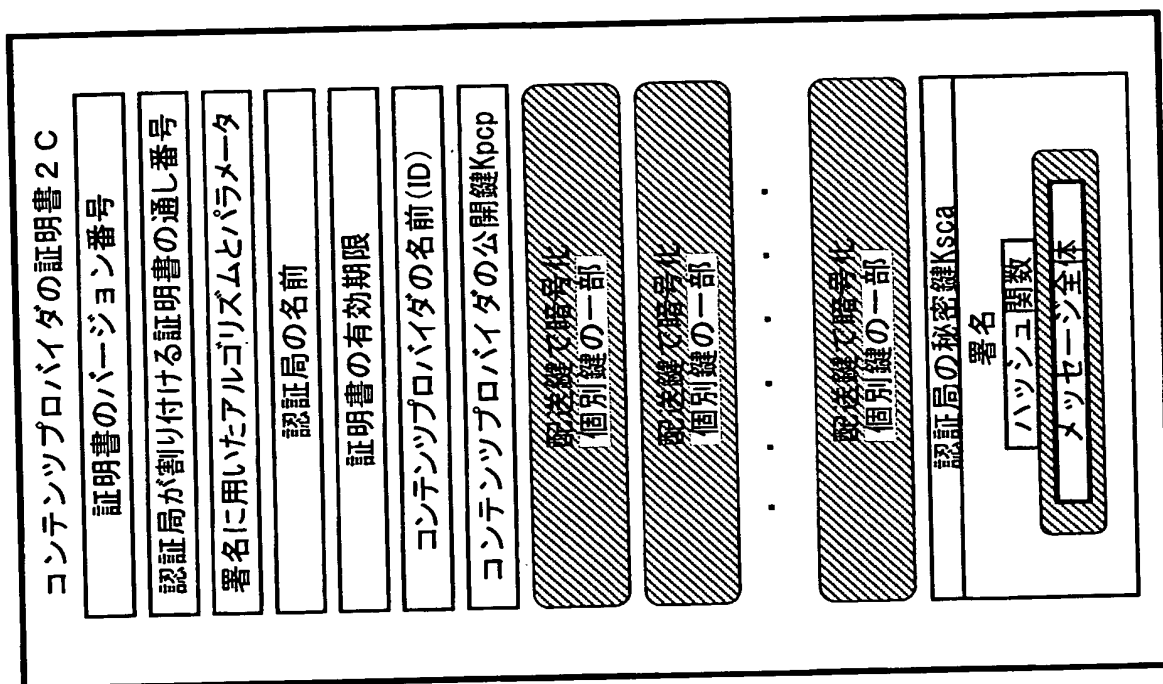


図 28

**THIS PAGE BLANK (USPTO)**



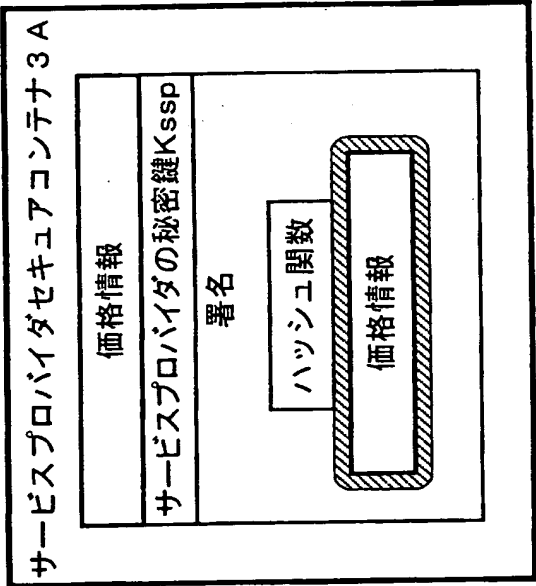


図 29

**THIS PAGE BLANK (USPTO)**

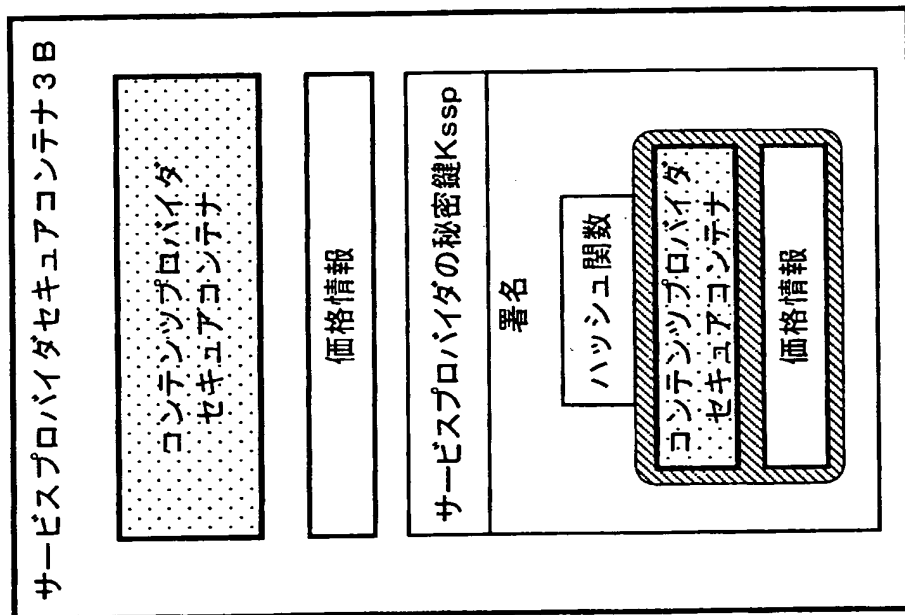


図30

**THIS PAGE BLANK (USPTO)**

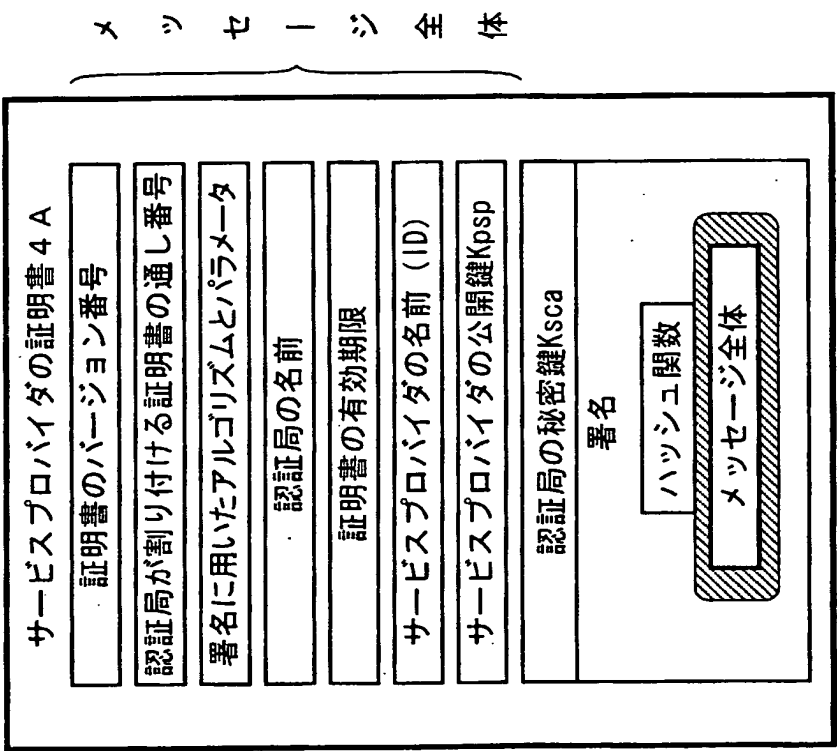


図 3 1

**THIS PAGE BLANK (USPTO)**

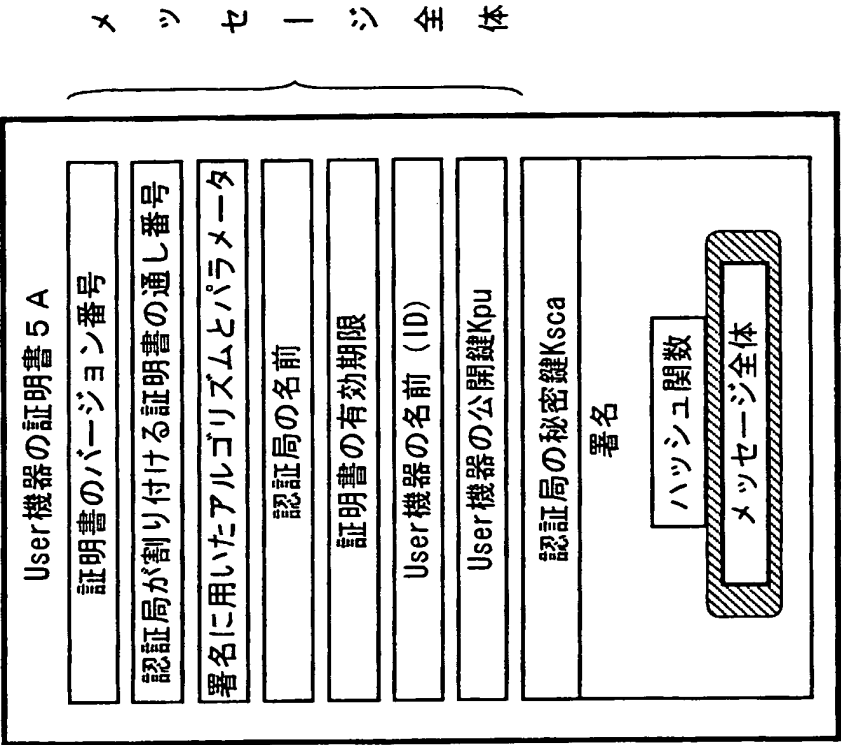


図 3 2

**THIS PAGE BLANK (USPTO)**



データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのID	
コンテンツプロバイダのID	
取扱方針のID	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
世代管理情報	
ルールの数	
ルールのアドレス情報	
ルール 1	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
⋮	⋮
ルール N	ルール番号（Rule#）
	利用権内容番号（Type）
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
（署名の検証の有無）	
公開鍵証明書	
署名	

図 3 3

**THIS PAGE BLANK (USPTO)**

データの種別	
取扱方針の種類 (アルバム)	
取扱方針の有効期限	
アルバムのID	
取扱方針のバージョン	
コンテンツプロバイダのID	
取扱方針のID	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針1
	⋮
	取扱方針N
世代管理情報	
ルール数	
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	コンテンツプロバイダの利益額
	コンテンツプロバイダの利益率
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 4

**THIS PAGE BLANK (USPTO)**

データの種別	
取扱方針の種類（シングル）	
取扱方針の有効期限	
コンテンツのID	
コンテンツプロバイダのID	
取扱方針のID	
取扱方針のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
世代管理情報	
ルールの数	
ルールアドレス情報	
ルール 1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
⋮	⋮
ルール N	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 5

**THIS PAGE BLANK (USPTO)**

データの種別	
取扱方針の種類 (アルバム)	
取扱方針の有効期限	
アルバムのID	
取扱方針のバージョン	
コンテンツプロバイダのID	
取扱方針のID	
地域コード	
使用可能機器条件	
使用可能User条件	
サービスプロバイダのID	
シングルコンテンツの取扱方針の数	
シングルコンテンツの取扱方針のアドレス情報	
シングル	取扱方針1
	⋮
	取扱方針N
世代管理情報	
ルール数	
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	利用権内容番号 (Type)
	パラメータ
	最低販売価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 6

**THIS PAGE BLANK (USPTO)**



データの種別	
価格情報の種類（シングル）	
価格情報の有効期限	
コンテンツのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
ルールの数	
ルールアドレス情報	
ルール 1	ルール番号（Rule#）
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
⋮	⋮
ルール N	ルール番号（Rule#）
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
（署名の検出の有無）	
公開鍵証明書	
署名	

図 3 7

**THIS PAGE BLANK (USPTO)**

データの種別	
価格情報の種類 (アルバム)	
価格情報の有効期限	
アルバムのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報1
	⋮
	価格情報N
ルールの数	
ルールのアドレス情報	
ルール1	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	サービスプロバイダの利益額
	サービスプロバイダの利益率
	価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 38

**THIS PAGE BLANK (USPTO)**

データの種別	
価格情報の種類 (シングル)	
価格情報の有効期限	
コンテンツのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
ルールの数	
ルールアドレス情報	
ル ー ル 1	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
⋮	⋮
ル ー ル N	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 3 9

**THIS PAGE BLANK (USPTO)**

データの種別	
価格情報の種類（アルバム）	
価格情報の有効期限	
アルバムのID	
サービスプロバイダのID	
価格情報のID	
価格情報のバージョン	
地域コード	
使用可能機器条件	
使用可能User条件	
コンテンツプロバイダのID	
取扱方針のID	
シングルコンテンツの価格情報の数	
シングルコンテンツの価格情報のアドレス情報	
シングル	価格情報1
	⋮
	価格情報N
ルール数	
ルールアドレス情報	
ルール1	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
⋮	⋮
ルールN	ルール番号 (Rule#)
	価格
	データサイズ
	送信情報
(署名の検出の有無)	
公開鍵証明書	
署名	

図 40

**THIS PAGE BLANK (USPTO)**



データの種別
使用許諾条件情報の種類
使用許諾条件情報の有効期限
コンテンツの I D
アルバムの I D
暗号処理部の I D
ユーザの I D
コンテンツプロバイダの I D
取扱方針の I D
取扱方針のバージョン
サービスプロバイダの I D
価格情報の I D
価格情報のバージョン
使用許諾条件情報の I D
再生権（利用権）のルール番号
利用権内容番号
再生残り回数
再生権の有効期限
複製権（利用権）のルール番号
利用権内容番号
複製残り回数
世代管理情報
再生権を保有する暗号処理部の I D

図 4 1

**THIS PAGE BLANK (USPTO)**

データの種別
暗号処理部の I D
ユーザの I D
コンテンツの I D
コンテンツプロバイダの I D
取扱方針の I D
取扱方針のバージョン
サービスプロバイダの I D
価格情報の I D
価格情報のバージョン
使用許諾条件の I D
ルール番号 (Rule#)
コンテンツプロバイダの利益額／利益率
サービスプロバイダの利益額／利益率
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元の I D

図 4 2

**THIS PAGE BLANK (USPTO)**

データの種別
暗号処理部の I D
ユーザの I D
コンテンツの I D
コンテンツプロバイダの I D
取扱方針の I D
取扱方針のバージョン
サービスプロバイダの I D
価格情報の I D
価格情報のバージョン
使用許諾条件の I D
ルール番号 (Rule#)
世代管理情報
コンテンツプロバイダの設定した送信情報のデータサイズ
コンテンツプロバイダの設定した送信情報
サービスプロバイダの設定した送信情報のデータサイズ
サービスプロバイダの設定した送信情報
供給元の I D

図 4 3

**THIS PAGE BLANK (USPTO)**

利用権内容番号	利用権内容			
	権利	期間制限	回数制限	複製制限
(1)	再生権	なし	なし	—
(2)		あり	なし	—
(3)		あり	なし	—
(4)		なし	あり	—
(5)	複製権	なし	なし	なし
(6)		なし	あり	なし
(7)		なし	なし	SCMS
(8)		なし	あり	
(9) ~ (15)	予備			
(16)	権利内容変更権		—	
(17)	再購入権		—	
(18)	追加購入権		—	
(19)	管理移動権		—	

図 4 4

**THIS PAGE BLANK (USPTO)**



(A)	再生権の有効期限
(B)	再生権の有効期限
(C)	再生権の有効期限 日数及び時間
(D)	再生権の有効期限 再生回数
(E)	複製権の有効期限
(F)	複製権の有効期限 複製回数
(G)	複製権の有効期限
(H)	複製権の有効期限 複製回数
(I)	権利内容変更権の有効期限 旧ルール番号 新ルール番号
(J)	再購入権の有効期限 旧ルール番号 新ルール番号 最大再配信世代情報
(K)	追加購入権の有効期限 最小保有コンテンツ数 最大保有コンテンツ数
(L)	管理移動権の有効期限
(M)	コンテンツ購入権の有効期限 旧コンテンツのID 旧ルール番号 新ルール番号

図 4 5

**THIS PAGE BLANK (USPTO)**

データの種別
コンテンツの種類 (シングル)
コンテンツの有効期限
コンテンツのカテゴリー
コンテンツの I D
コンテンツプロバイダの I D
コンテンツの暗号方式
暗号化したコンテンツのデータ長
暗号化したコンテンツ
公開鍵証明書
署名

図 4 6

**THIS PAGE BLANK (USPTO)**

データの種別	
コンテンツの種類（アルバム）	
コンテンツの有効期限	
アルバムのID	
コンテンツプロバイダのID	
シングルコンテンツの数	
シングルコンテンツのアドレス情報	
シングル	コンテンツ1
	⋮
	コンテンツN
公開鍵証明書	
署名	

図 4 7

**THIS PAGE BLANK (USPTO)**

データの種別
鍵データの種類 (シングル)
鍵の有効期限
コンテンツの I D
コンテンツプロバイダの I D
鍵のバージョン
コンテンツ鍵の暗号方式
暗号化したコンテンツ鍵
個別鍵の暗号方式
暗号化した個別鍵
公開鍵証明書
署名

図 4 8

**THIS PAGE BLANK (USPTO)**



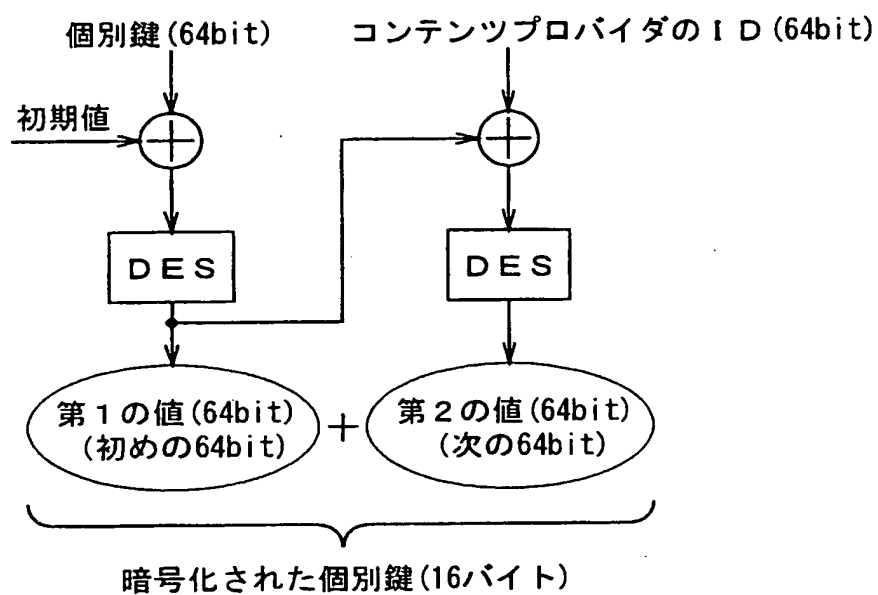


図 4 9

**THIS PAGE BLANK (USPTO)**

データの種別	
鍵データの種類（アルバム）	
鍵の有効期限	
アルバムのID	
コンテンツプロバイダID	
鍵のバージョン	
シングルコンテンツ用の鍵データの数	
シングルコンテンツ用の鍵データのアドレス情報	
シングル	鍵データ 1
	⋮
	鍵データ N
公開鍵証明書	
署名	

図 5 0

**THIS PAGE BLANK (USPTO)**

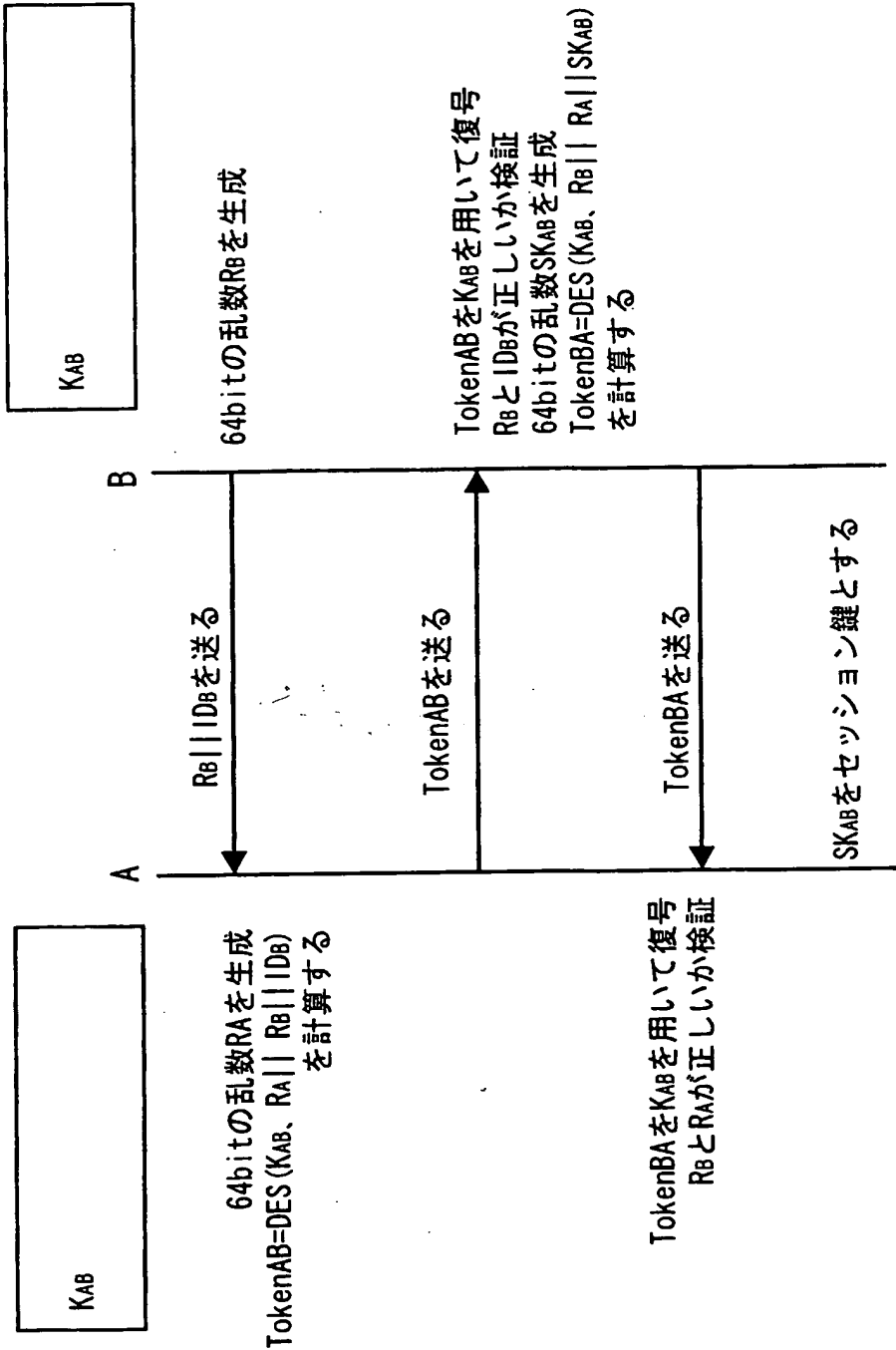


図 5 1

**THIS PAGE BLANK (USPTO)**

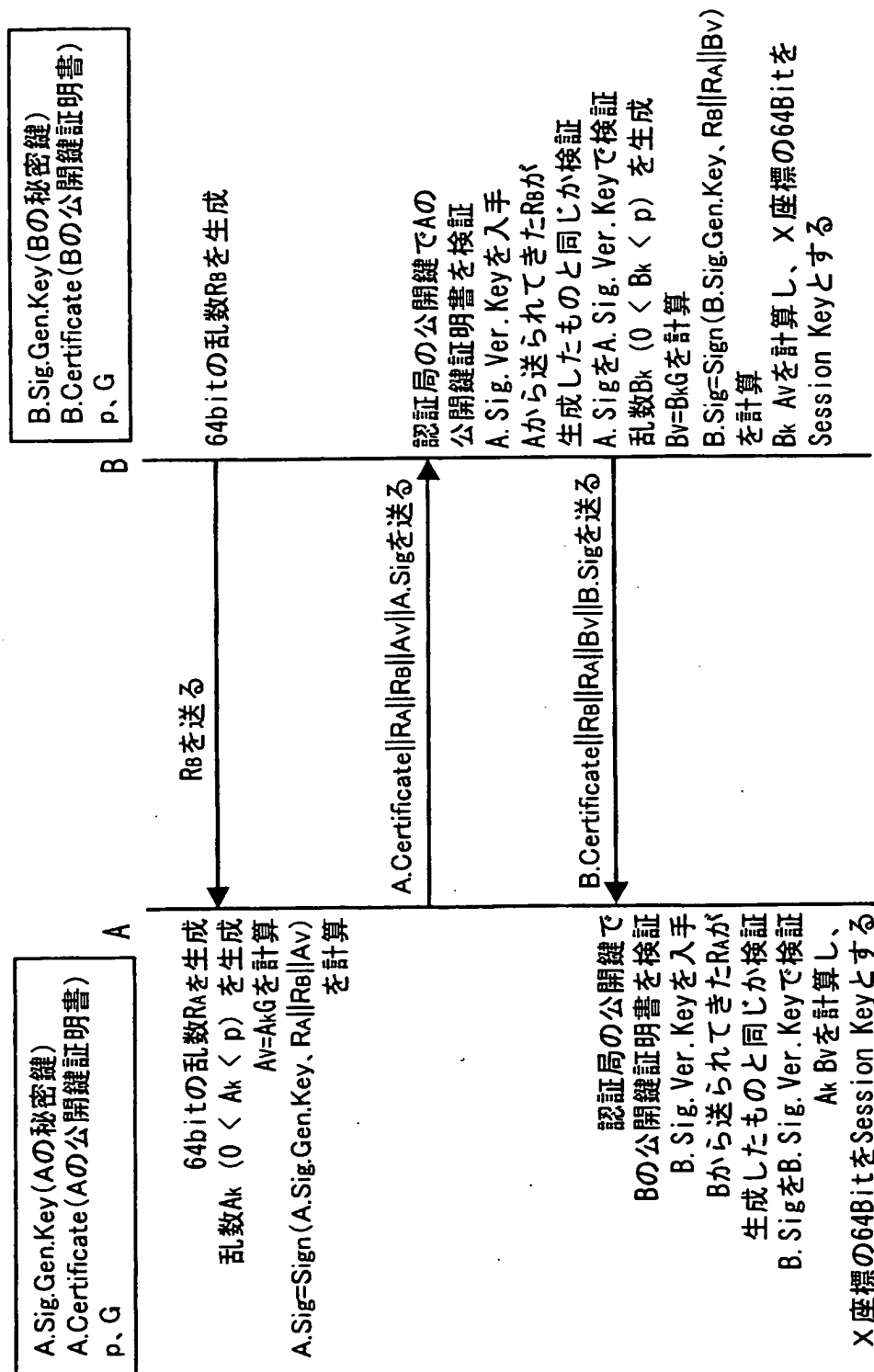
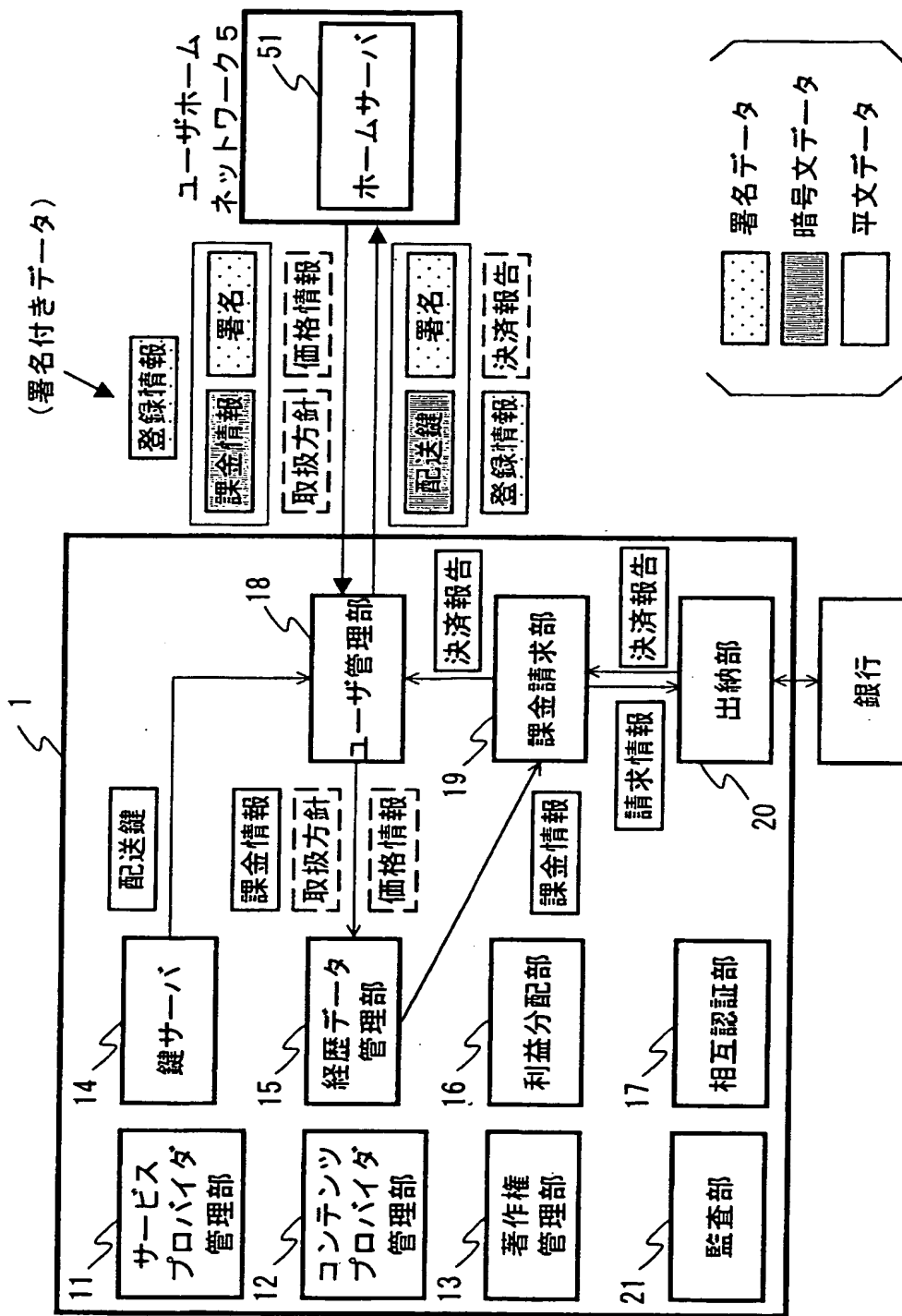


図 5 2

**THIS PAGE BLANK (USPTO)**





**THIS PAGE BLANK (USPTO)**

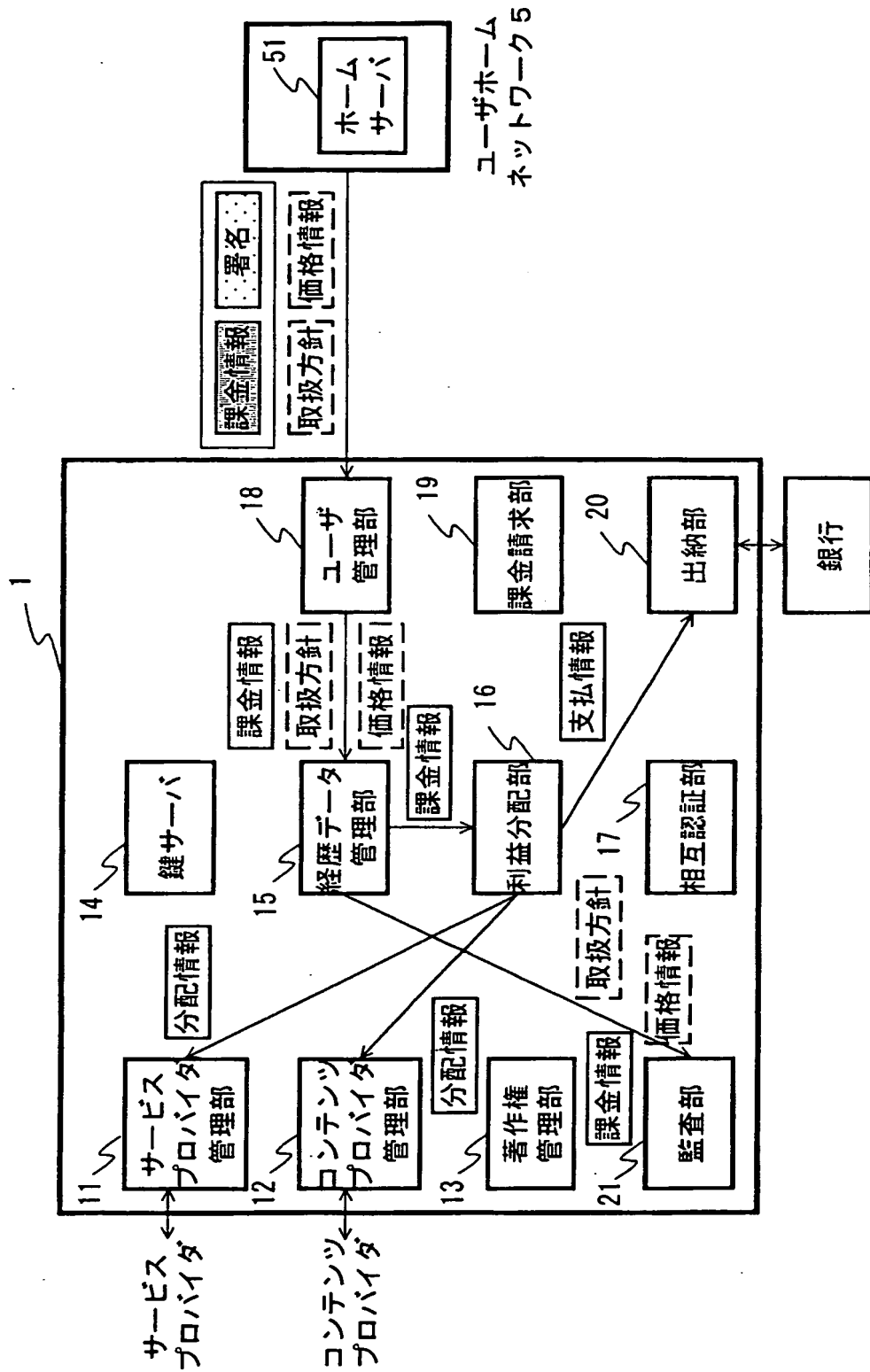


図 5 4

**THIS PAGE BLANK (USPTO)**

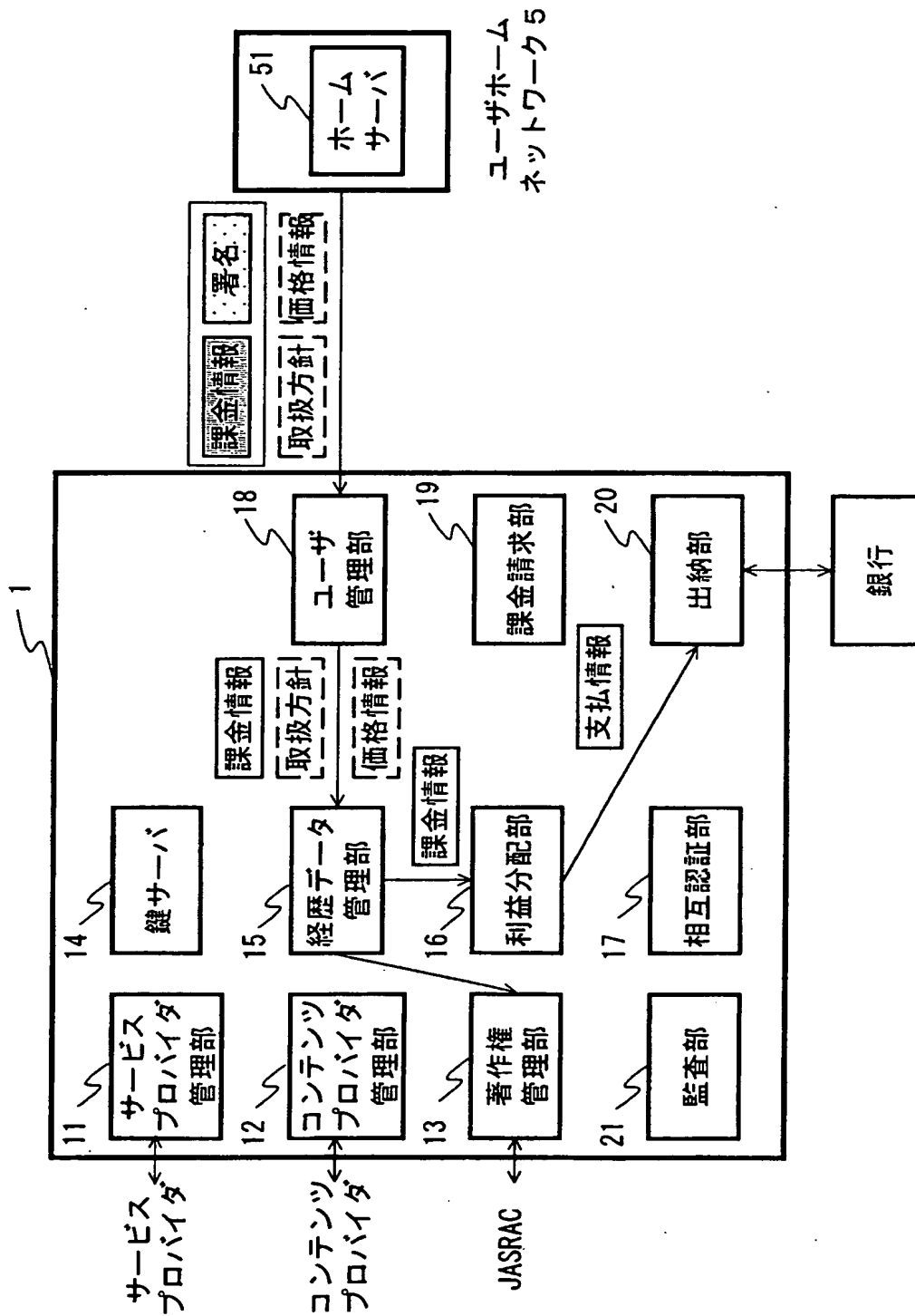


図 55

**THIS PAGE BLANK (USPTO)**

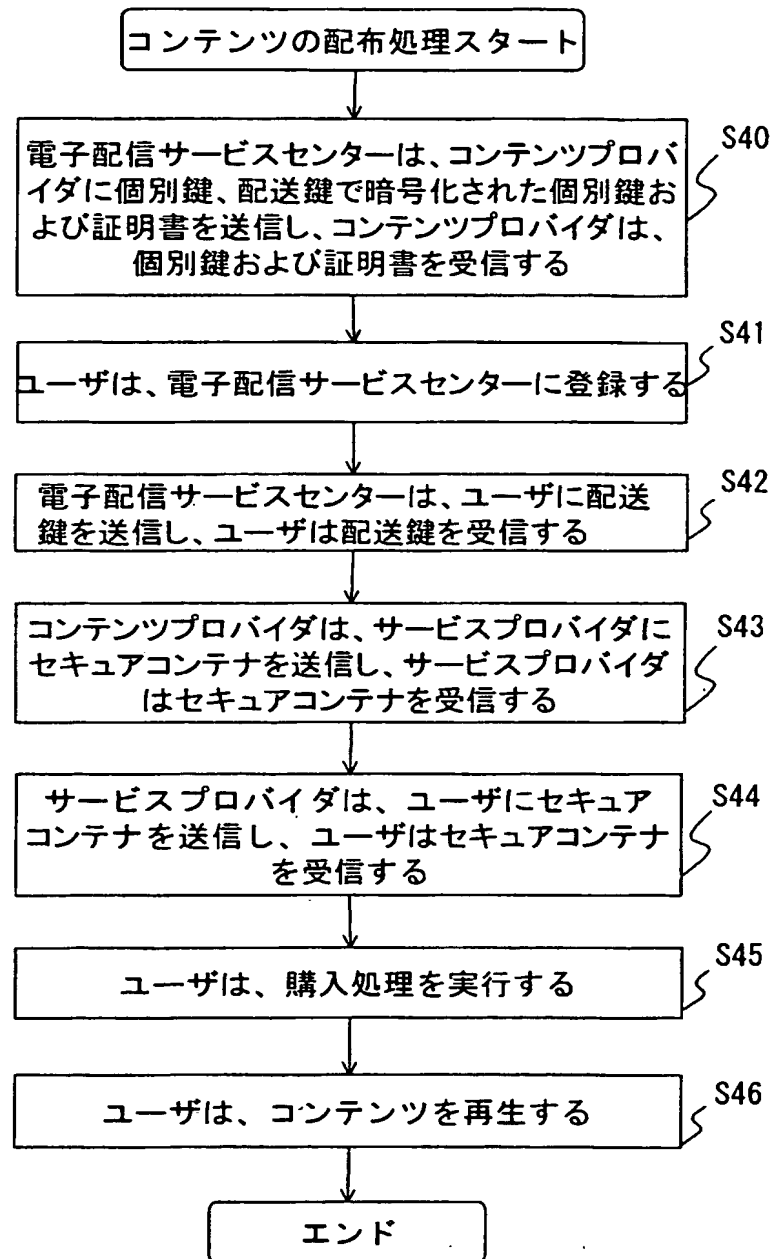


図 5 6

**THIS PAGE BLANK (USPTO)**



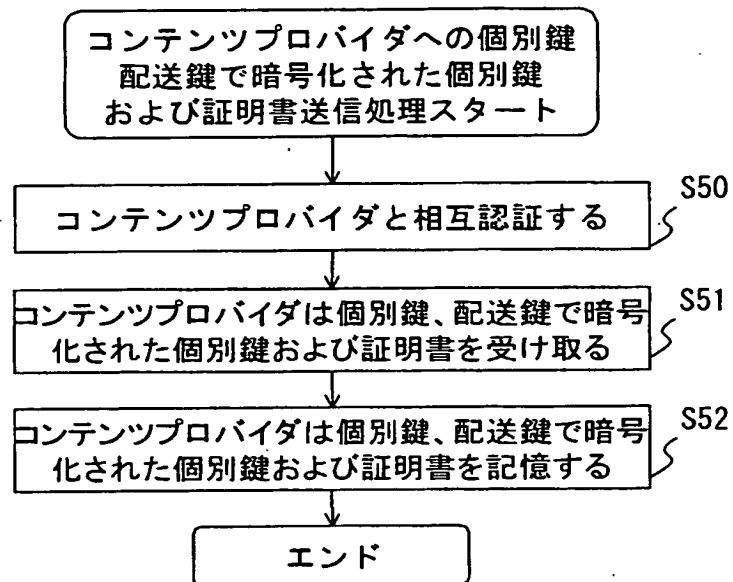


図 5 7

**THIS PAGE BLANK (USPTO)**

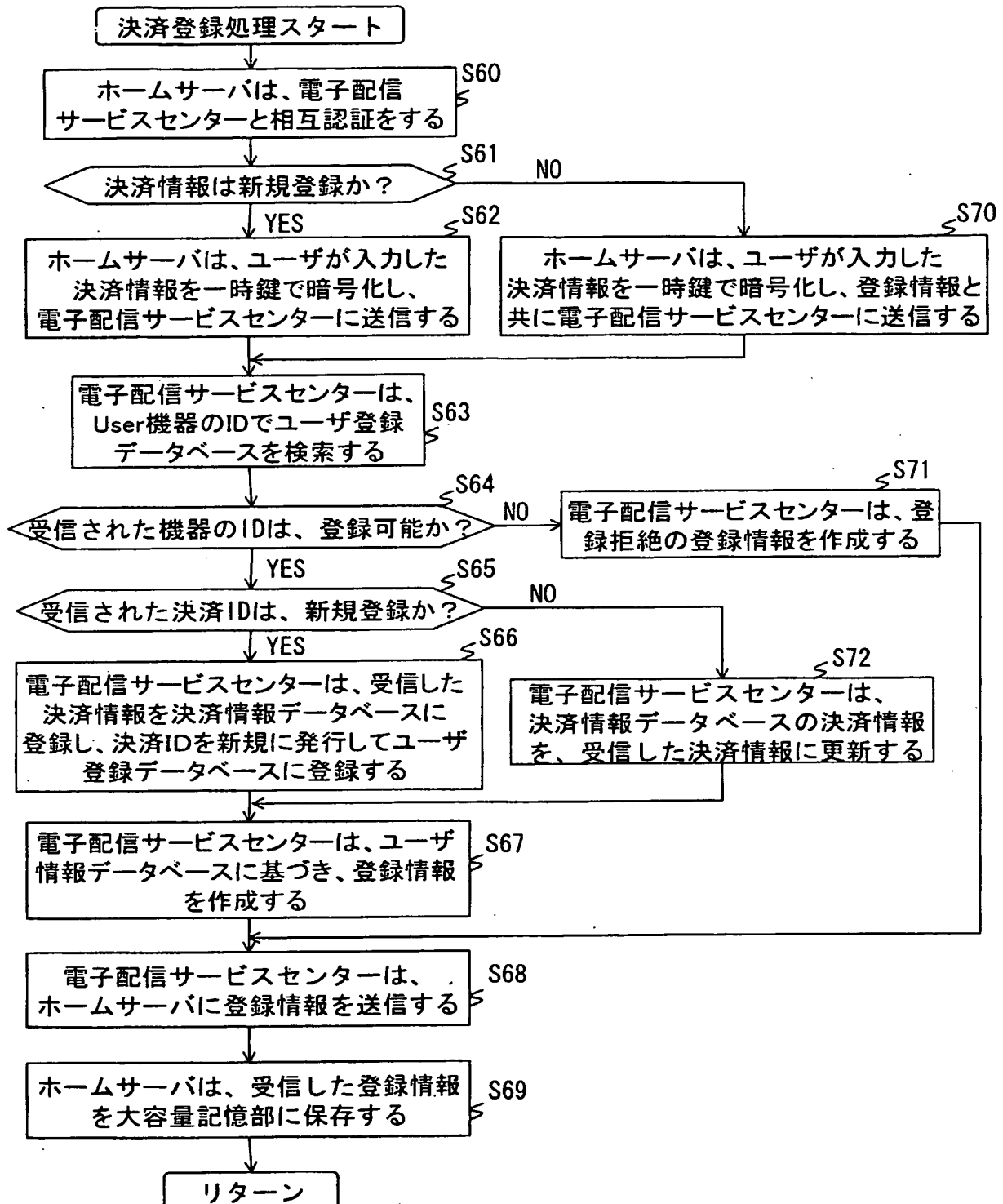


図 58

**THIS PAGE BLANK (USPTO)**

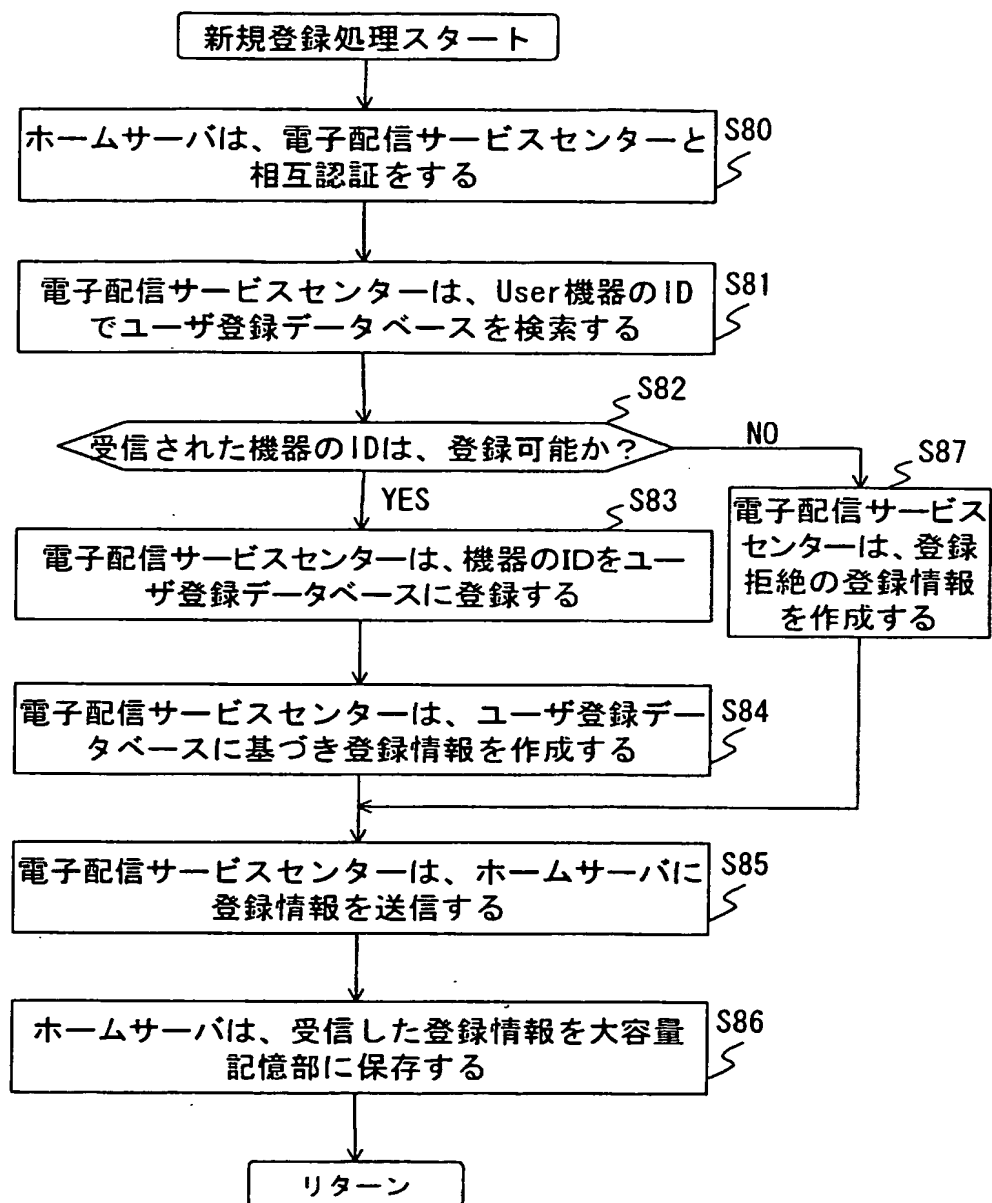


図 5 9

**THIS PAGE BLANK (USPTO)**

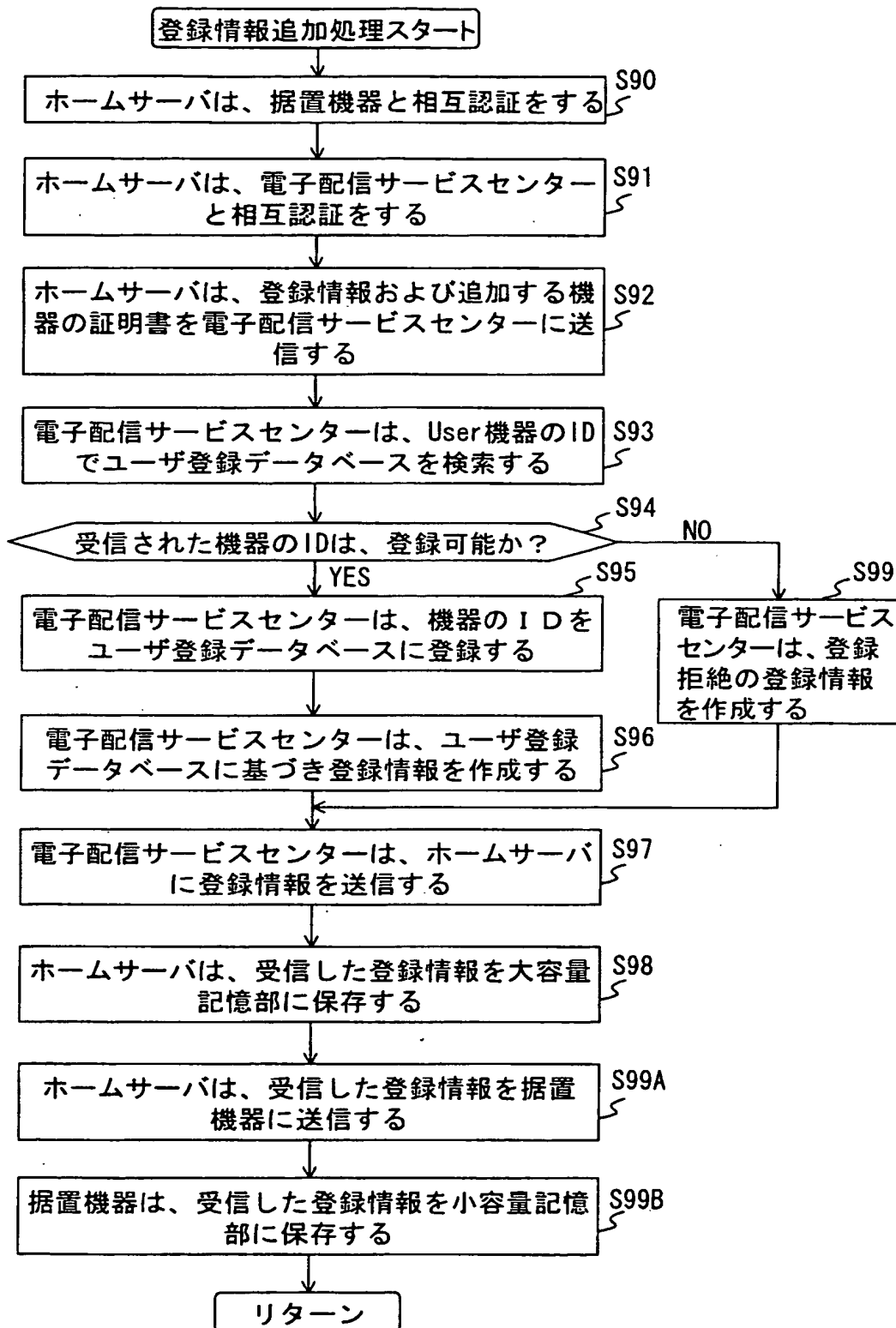


図 60

**THIS PAGE BLANK (USPTO)**



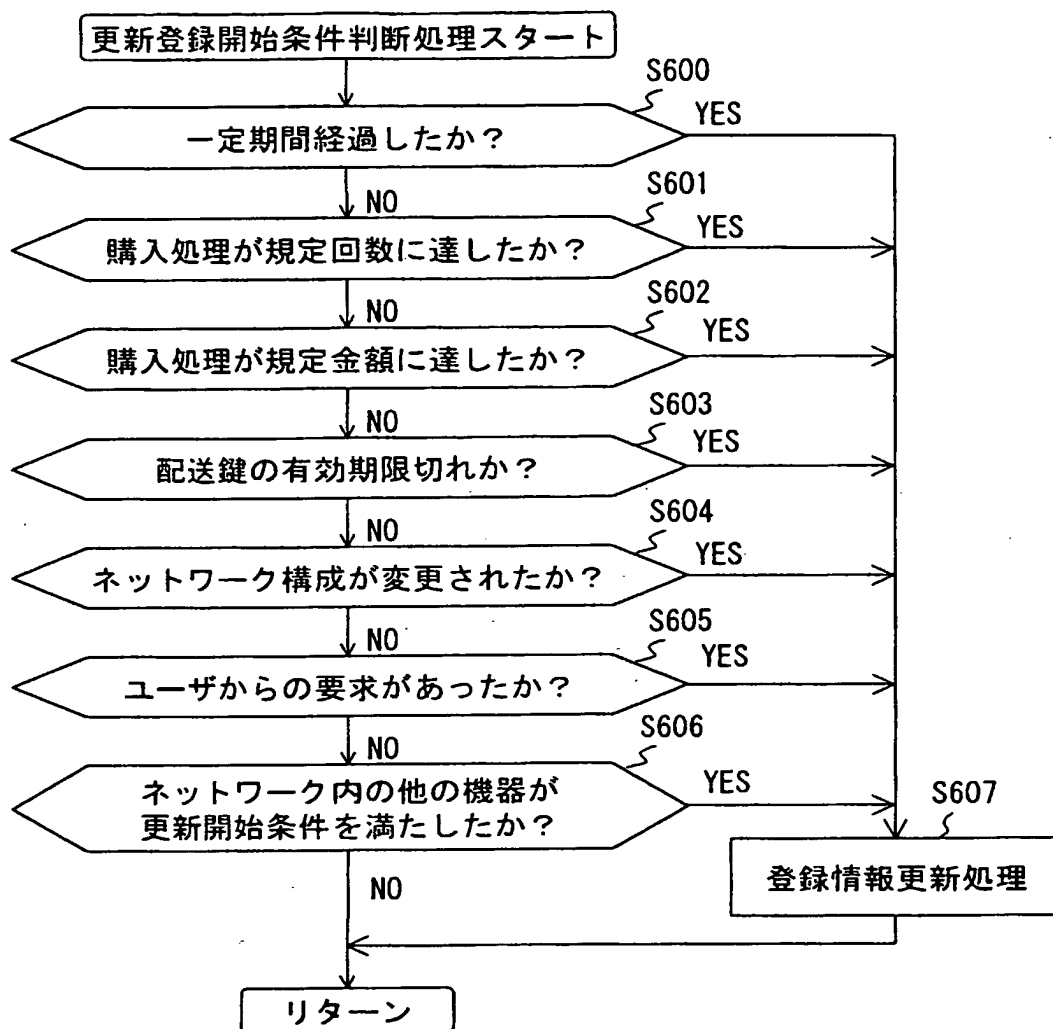


図 6 1

**THIS PAGE BLANK (USPTO)**

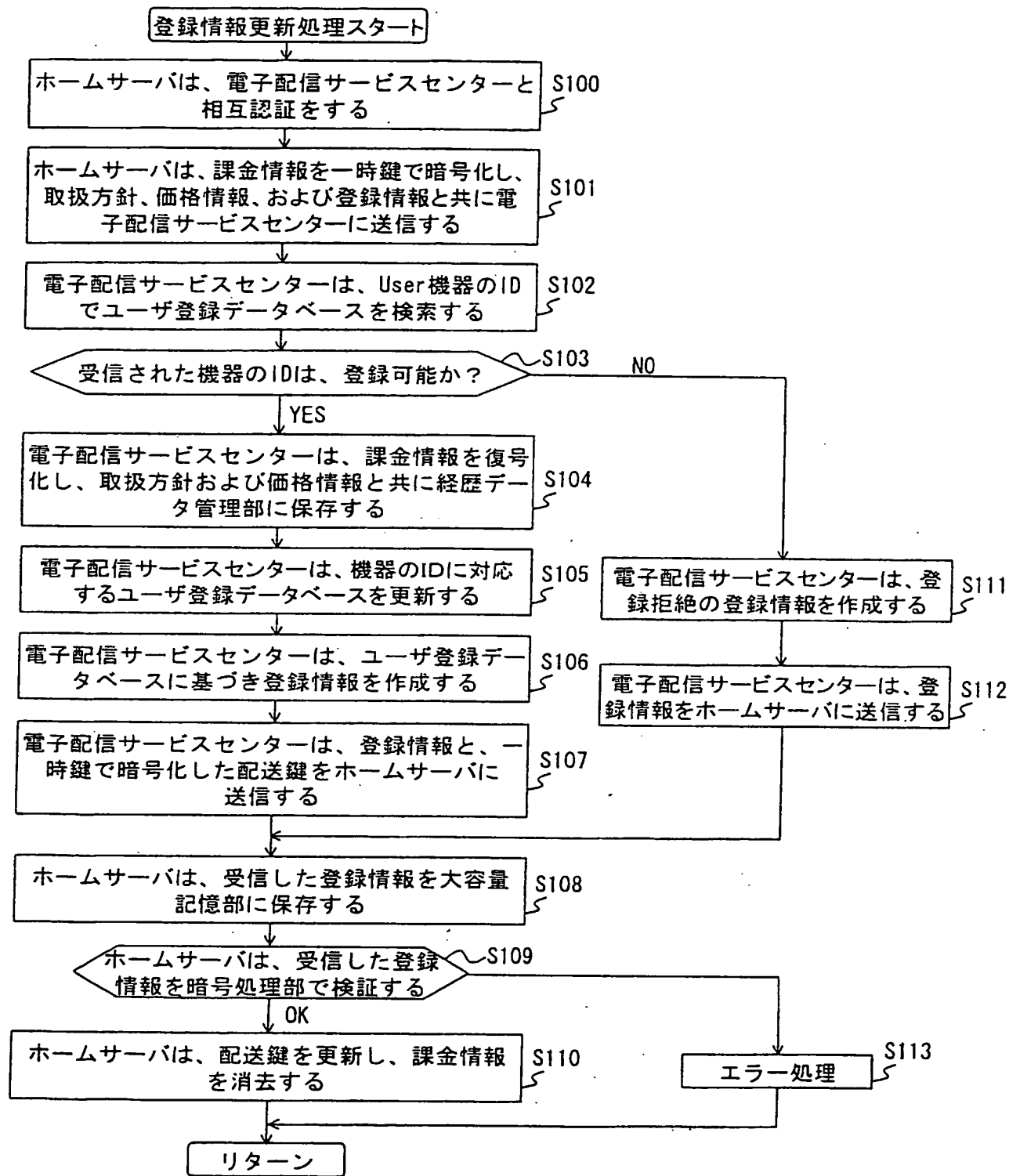


図 6 2

**THIS PAGE BLANK (USPTO)**

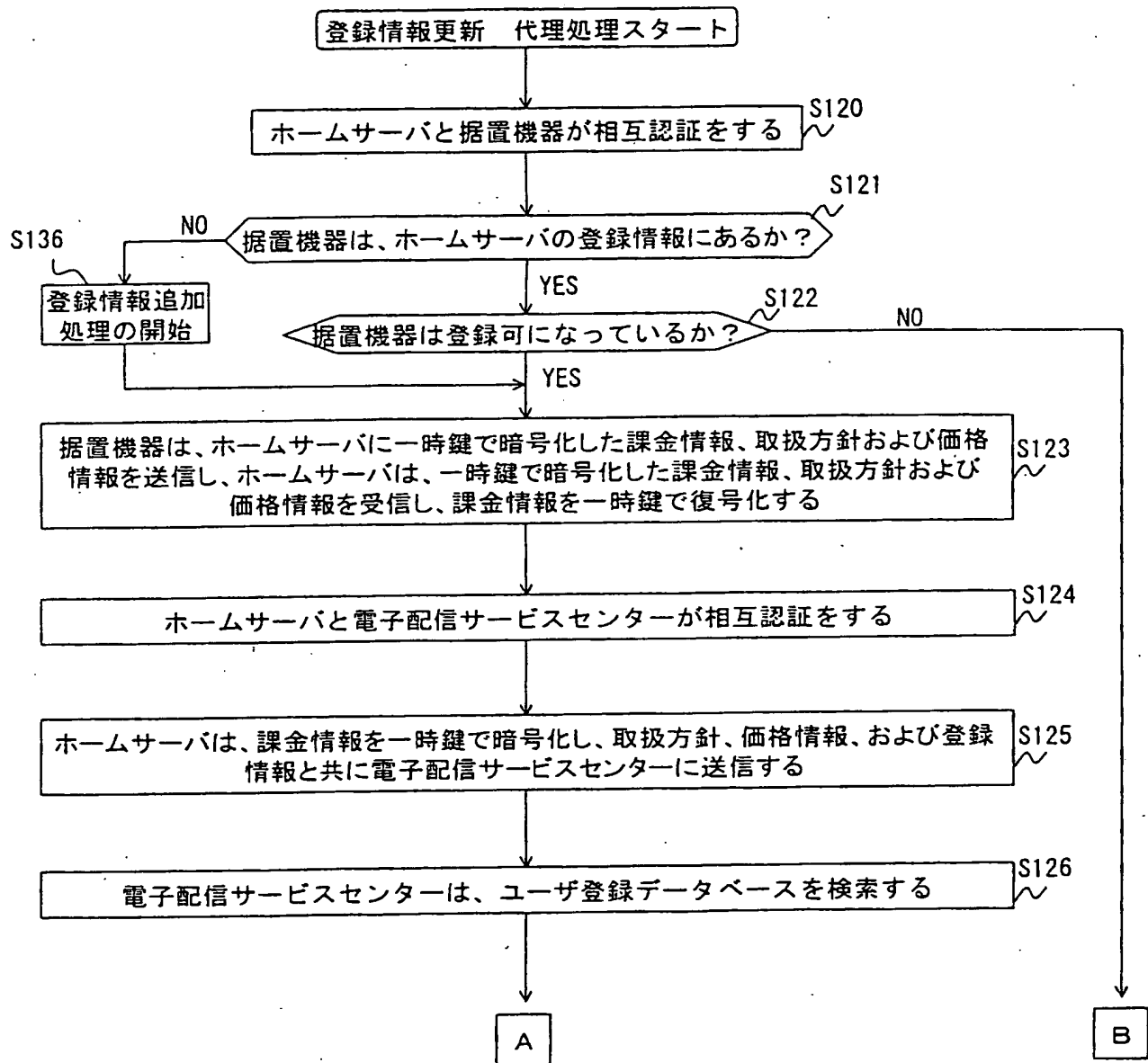


図 6 3

**THIS PAGE BLANK (USPTO)**

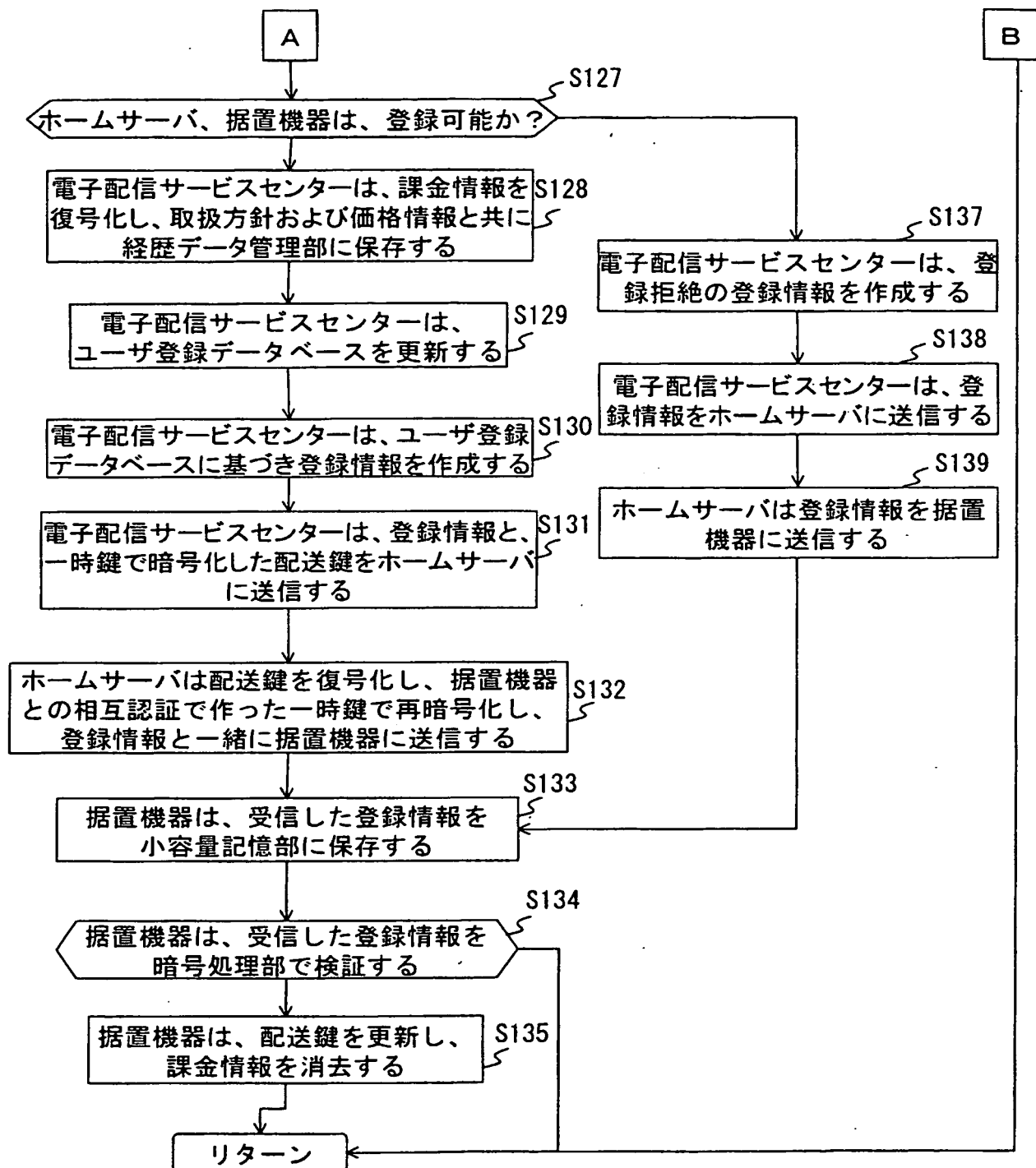


図 6 4

**THIS PAGE BLANK (USPTO)**



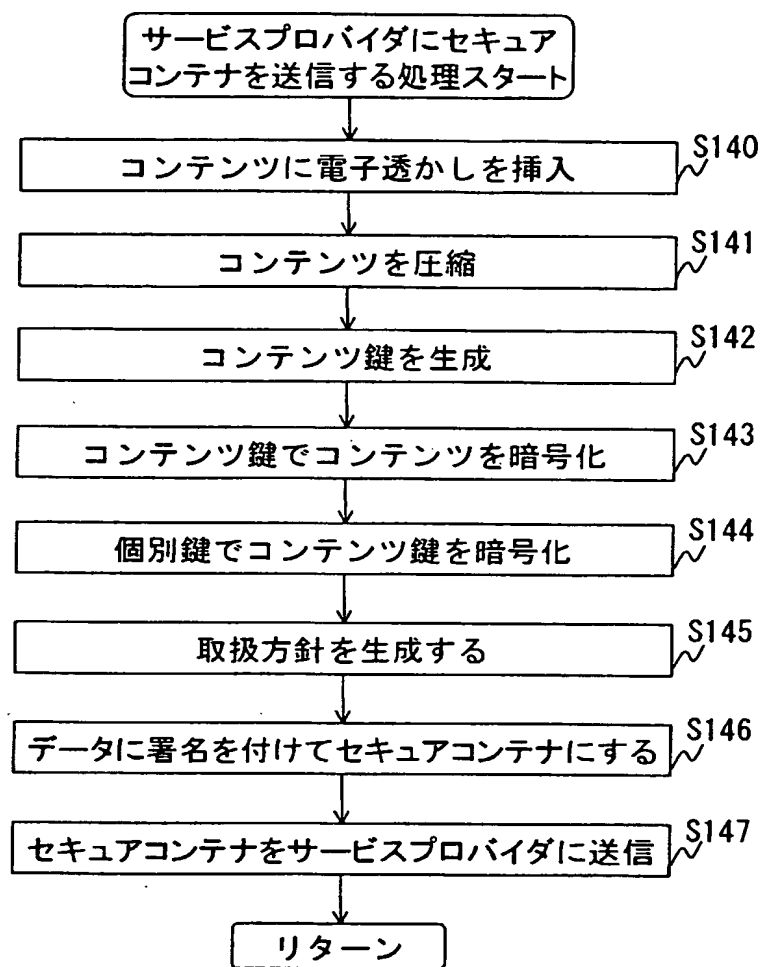


図 6 5

**THIS PAGE BLANK (USPTO)**

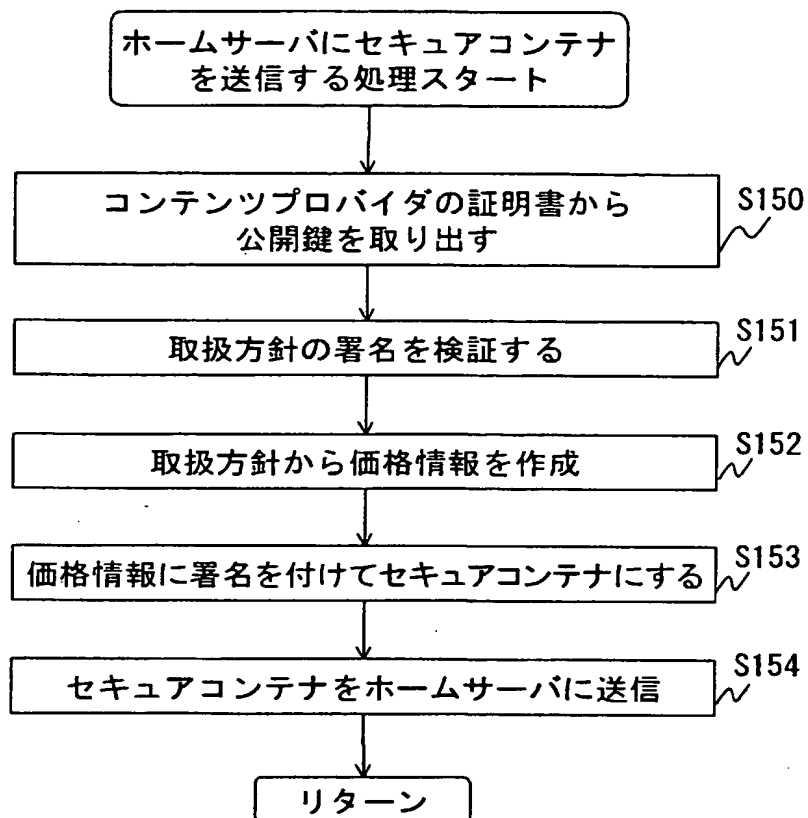


図 6 6

**THIS PAGE BLANK (USPTO)**

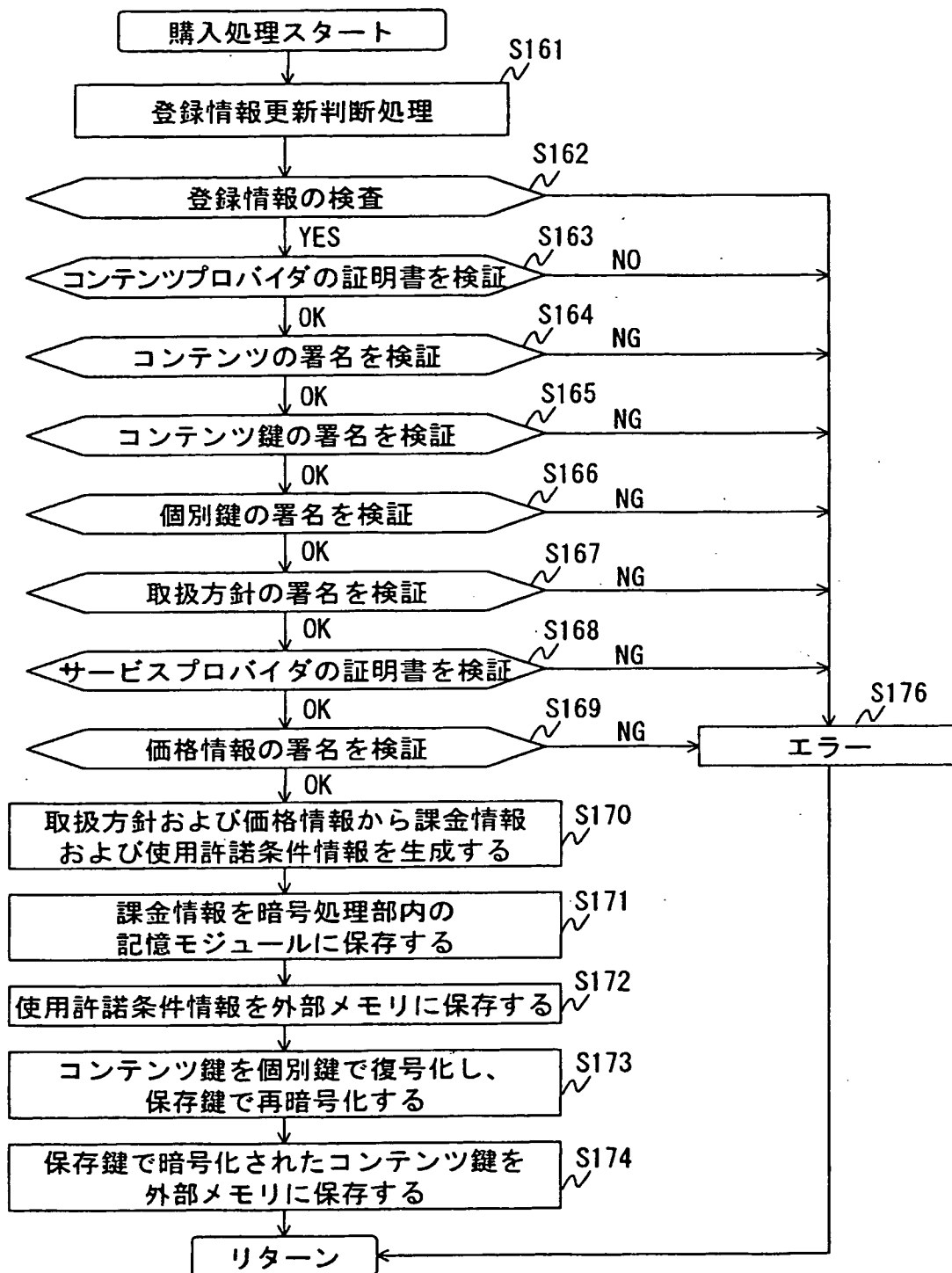


図 67

**THIS PAGE BLANK (USPTO)**

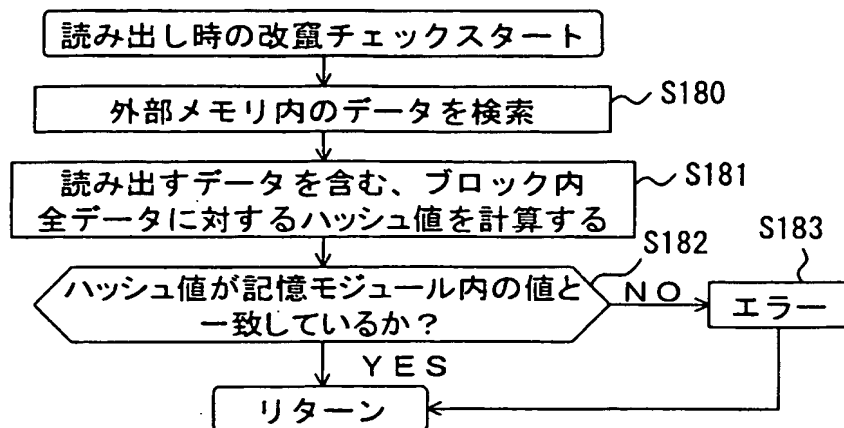


図 6 8

**THIS PAGE BLANK (USPTO)**



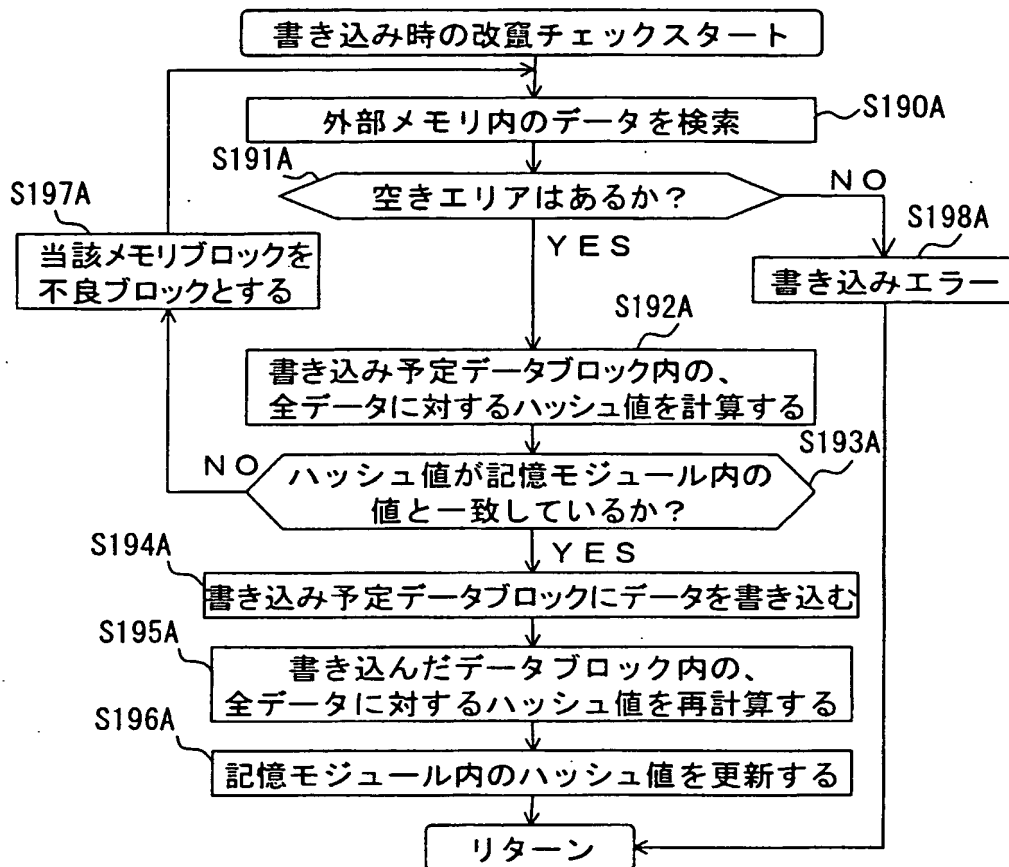


図 6 9

**THIS PAGE BLANK (USPTO)**

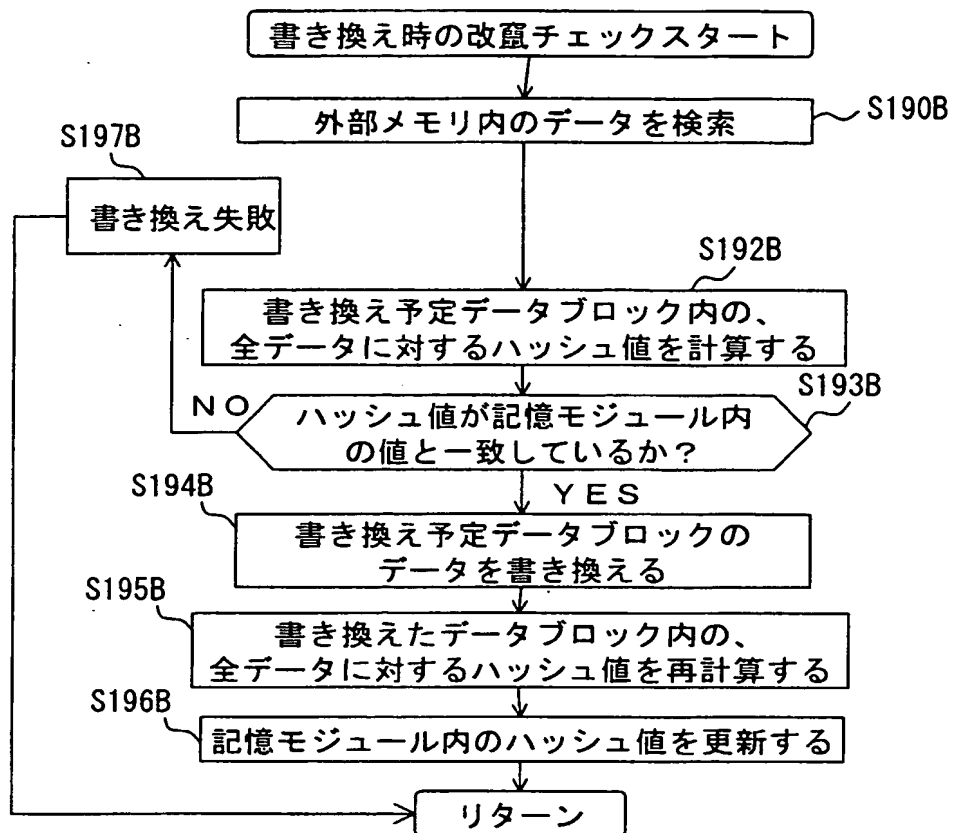


図 70

**THIS PAGE BLANK (USPTO)**

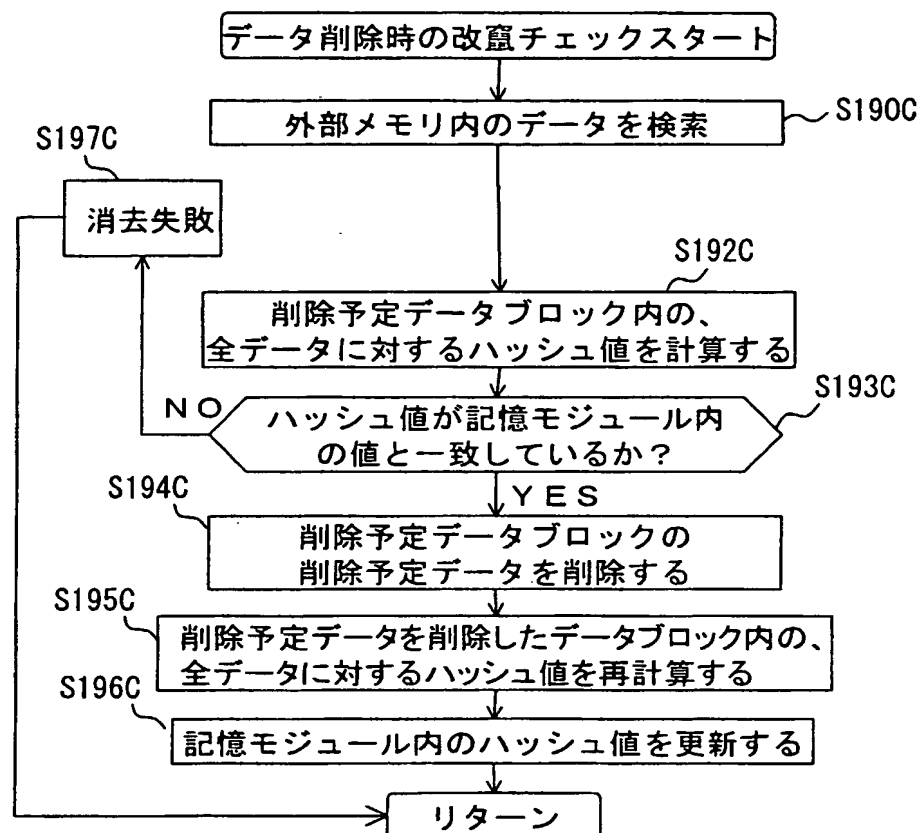


図 7 1

**THIS PAGE BLANK (USPTO)**

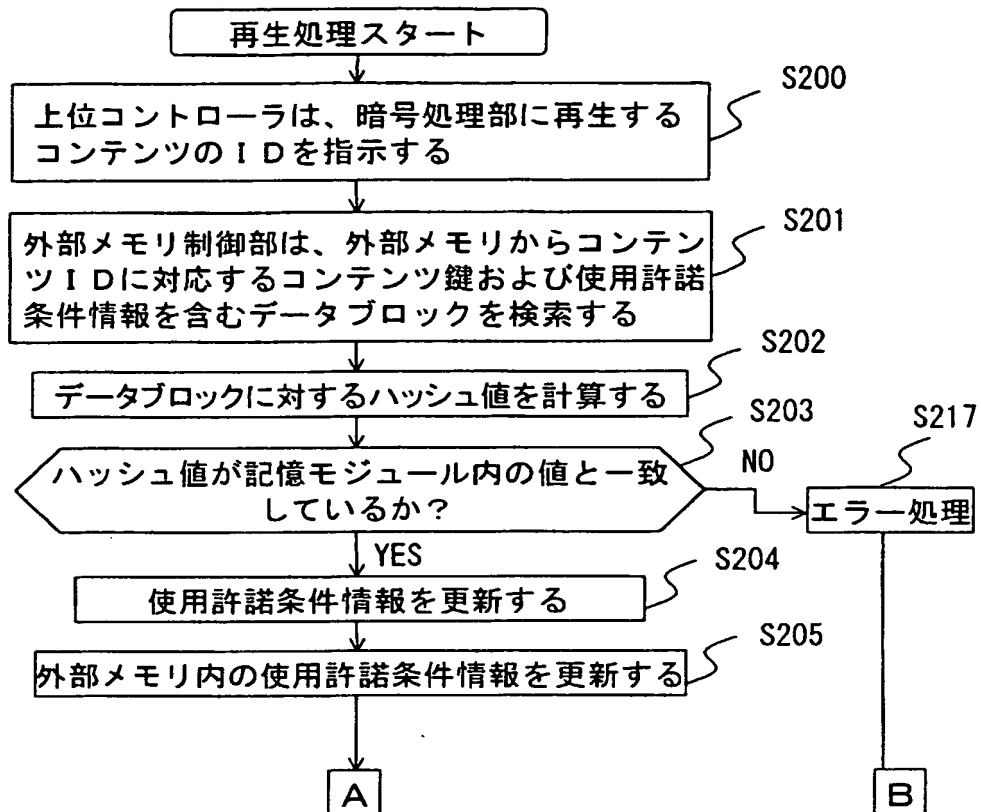


図 7 2

**THIS PAGE BLANK (USPTO)**



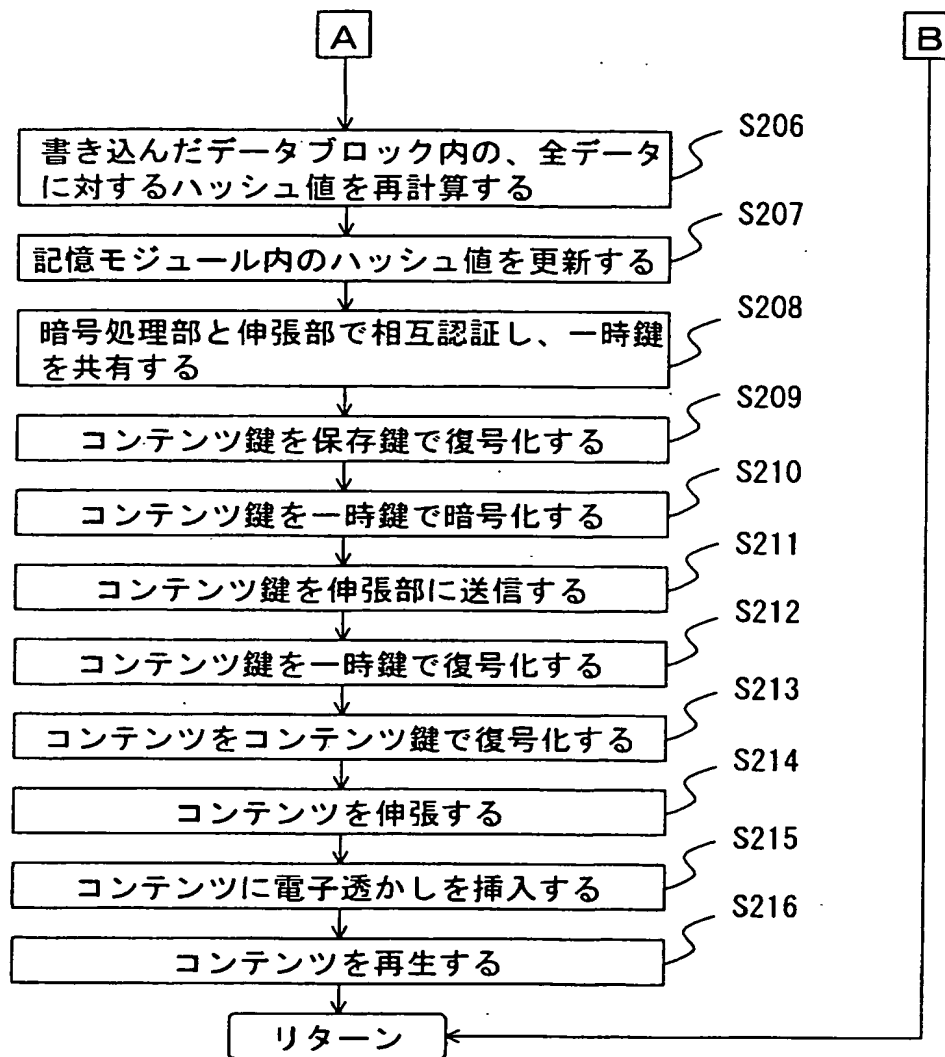


図 7 3

**THIS PAGE BLANK (USPTO)**

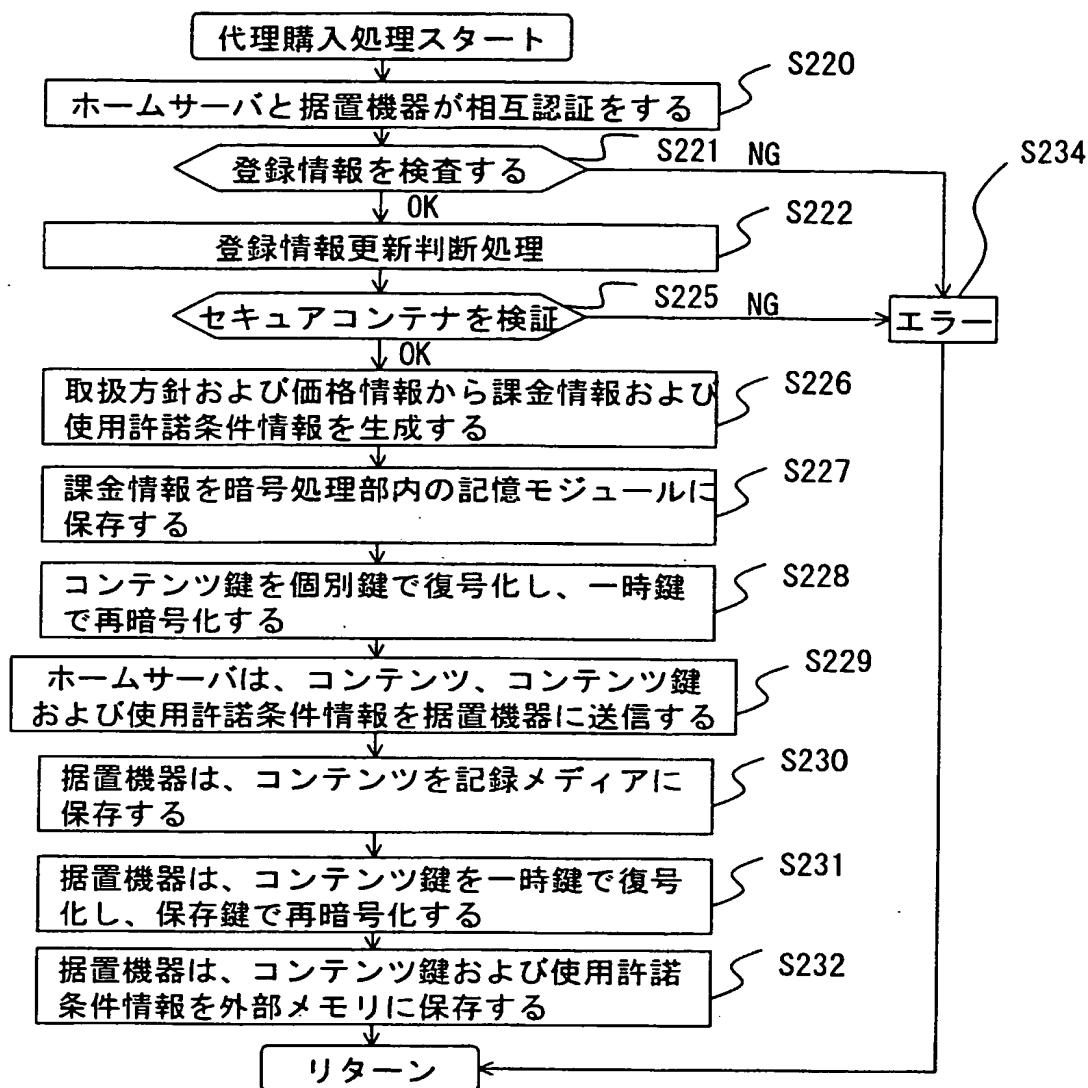


図 7 4

**THIS PAGE BLANK (USPTO)**

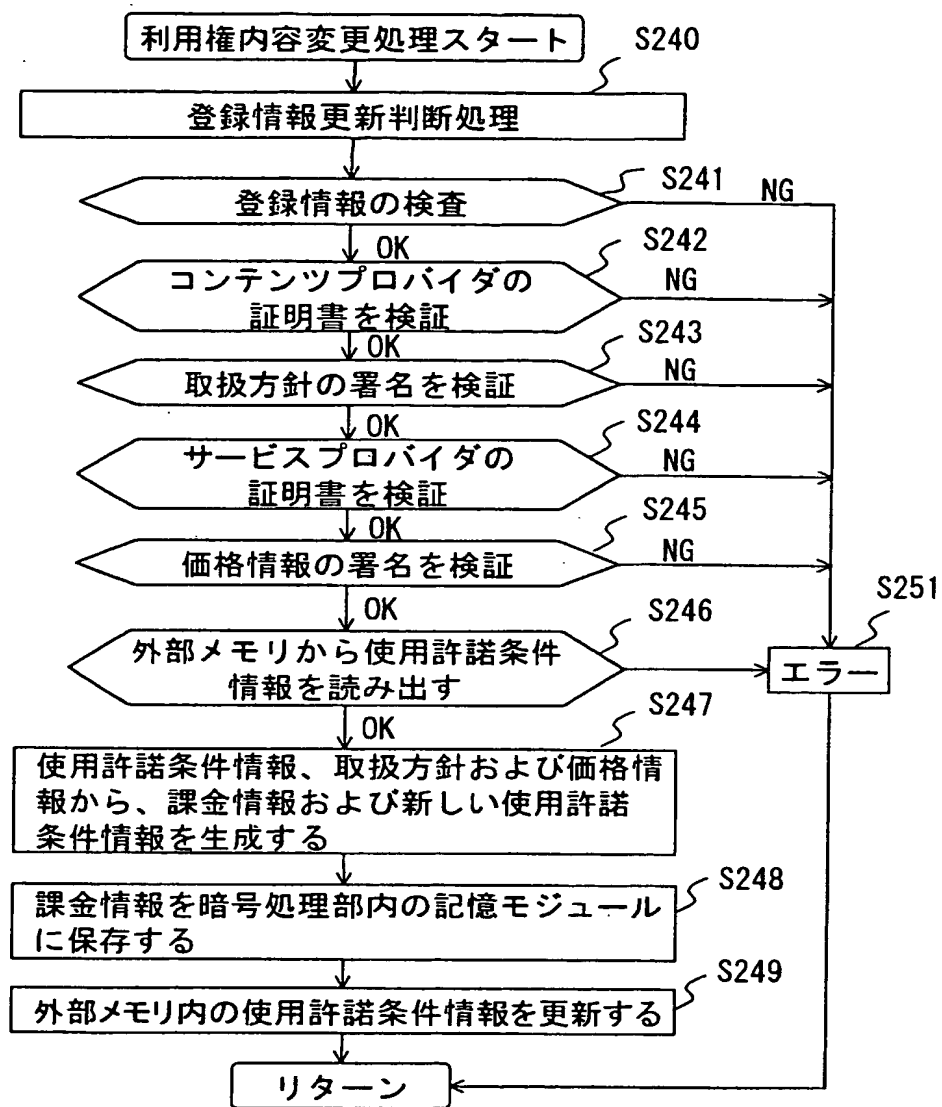


図 7 5

**THIS PAGE BLANK (USPTO)**

ルール n	ルール番号
	利用権内容番号
	パラメータ
	最低価格
	取り分（利益率）
ルール 1	ルール番号 # 1
	利用権内容番号 # 1
	なし
	¥ 3 5 0
	3 0 %
ルール 2	ルール番号 # 2
	利用権内容番号 # 2
	1 時間
	¥ 1 0 0
	3 0 %
ルール 3	ルール番号 # 3
	利用権内容番号 # 6
	1 回
	¥ 3 0
	3 0 %
ルール 4	ルール番号 # 4
	利用権内容番号 # 1 3
	# 2 / # 1
	¥ 2 0 0
	2 0 %
ルール 5	ルール番号 # 5
	利用権内容番号 # 1 4
	# 1 / # 1
	¥ 2 5 0
	2 0 %

図 7 6

**THIS PAGE BLANK (USPTO)**



ル ー ル n	ルール番号
	パラメータ
	価格
ル ー ル 1	ルール番号 # 1
	3 0 %
	¥ 5 0 0
ル ー ル 2	ルール番号 # 2
	4 0 %
	¥ 1 0 0
ル ー ル 3	ルール番号 # 3
	4 0 %
	¥ 1 0 0
ル ー ル 4	ルール番号 # 4
	1 0 %
	¥ 2 0 0
ル ー ル 5	ルール番号 # 5
	2 0 %
	¥ 3 5 0

図 7 7

**THIS PAGE BLANK (USPTO)**

ルール 1	# 1
	# 1
	なし
	¥ 3 5 0
	3 0 %
ルール 2	# 2
	# 2
	1 時間
	¥ 1 0 0
	3 0 %
ルール 3	# 3
	# 1 3
	# 2 / # 1
	¥ 2 0 0
	2 0 %

取扱方針のルール部の一部

ルール 1	# 1
	3 0 %
	¥ 5 0 0
ルール 2	# 2
	4 0 %
	¥ 1 0 0
ルール 3	# 3
	1 0 %
	¥ 2 0 0

価格情報のルール部の一部

現在

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	# 2
	# 2
	3 0 分 / 2 時間

使用許諾条件情報のルール部

変更後

ルール	ルール番号
	利用権内容番号
	パラメータ
ルール	# 1
	# 1
	なし

使用許諾条件情報のルール部

図 7 8

**THIS PAGE BLANK (USPTO)**

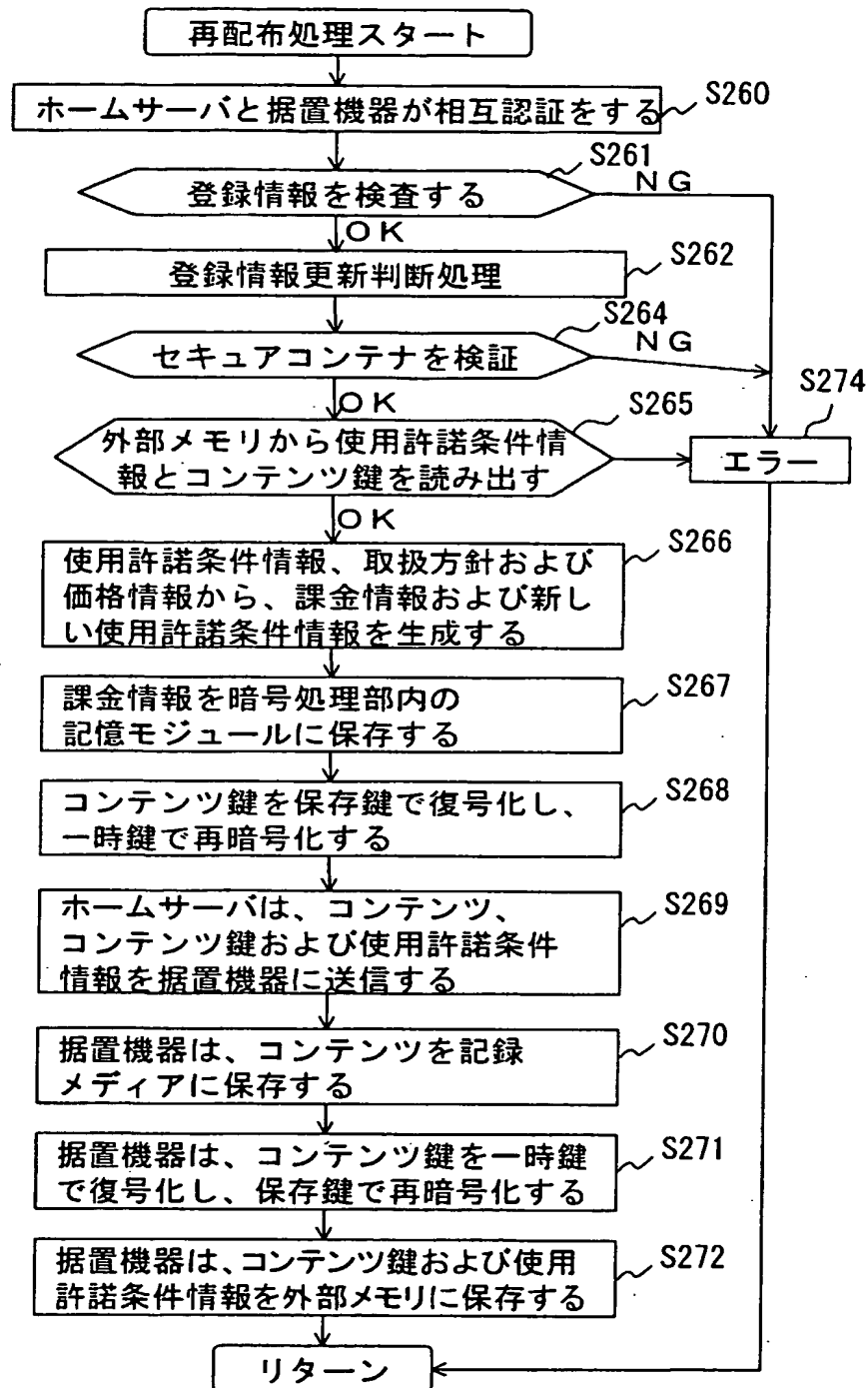


図 7 9

**THIS PAGE BLANK (USPTO)**

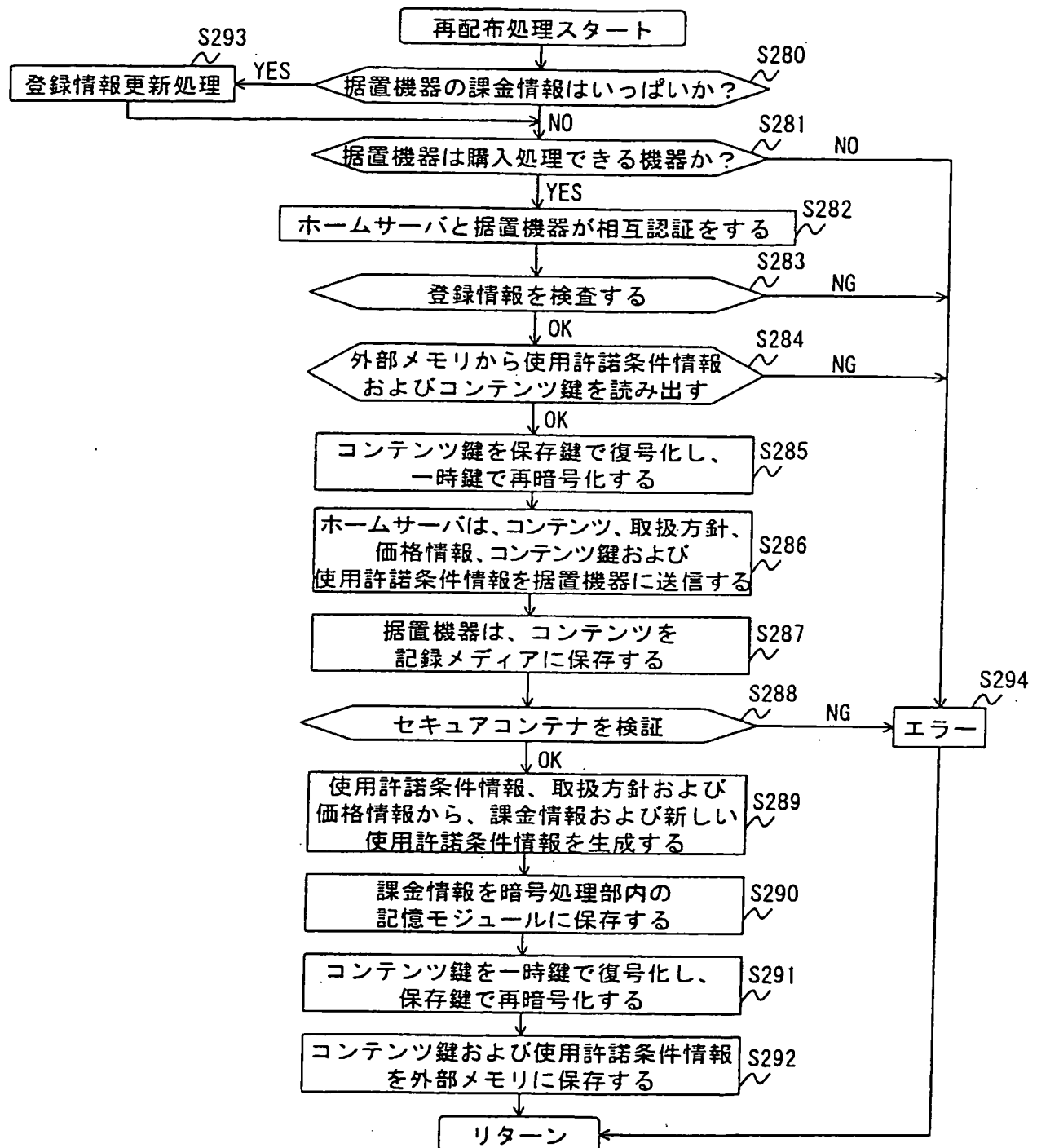


図 80

**THIS PAGE BLANK (USPTO)**



ル ー ル 1	ルール番号 # 1
	利用権内容番号 # 1
	なし
	¥ 3 5 0
	3 0 %
ル ー ル 2	ルール番号 # 2
	利用権内容番号 # 1 6
	なし
	¥ 1 0 0
	5 0 %

取扱方針のルール部の一部

ル ー ル 1	ルール番号 # 1
	3 0 %
	¥ 5 0 0
ル ー ル 2	ルール番号 # 2
	0 %
	¥ 1 0 0

価格情報のルール部の一部

(a) ル ー ル	ルール番号 # 1	(ルール番号)
	ID 1	(暗号処理部のID)
	なし	—— (再生権を保有する暗号処理部のID)



初期状態：  
再生権、時間・回数制限なし、管理移動権なし

(b) ル ー ル	ルール番号 # 1	管理移動権を購入後： 再生権、時間・回数制限なし 管理移動権あり（購入者／保持者）
	ID 1	
	あり ID 1	



(c) ル ー ル	ルール番号 # 1	管理移動権を移動後： 送信側（ID 1）の使用許諾条件 情報状態の一部
	ID 1	
	あり ID 2	

ル ー ル	ルール番号 # 1	管理移動権を移動後： 受信側（ID 2）の使用許諾条件 情報状態の一部
	ID 1	
	あり ID 2	

図 8 1

**THIS PAGE BLANK (USPTO)**

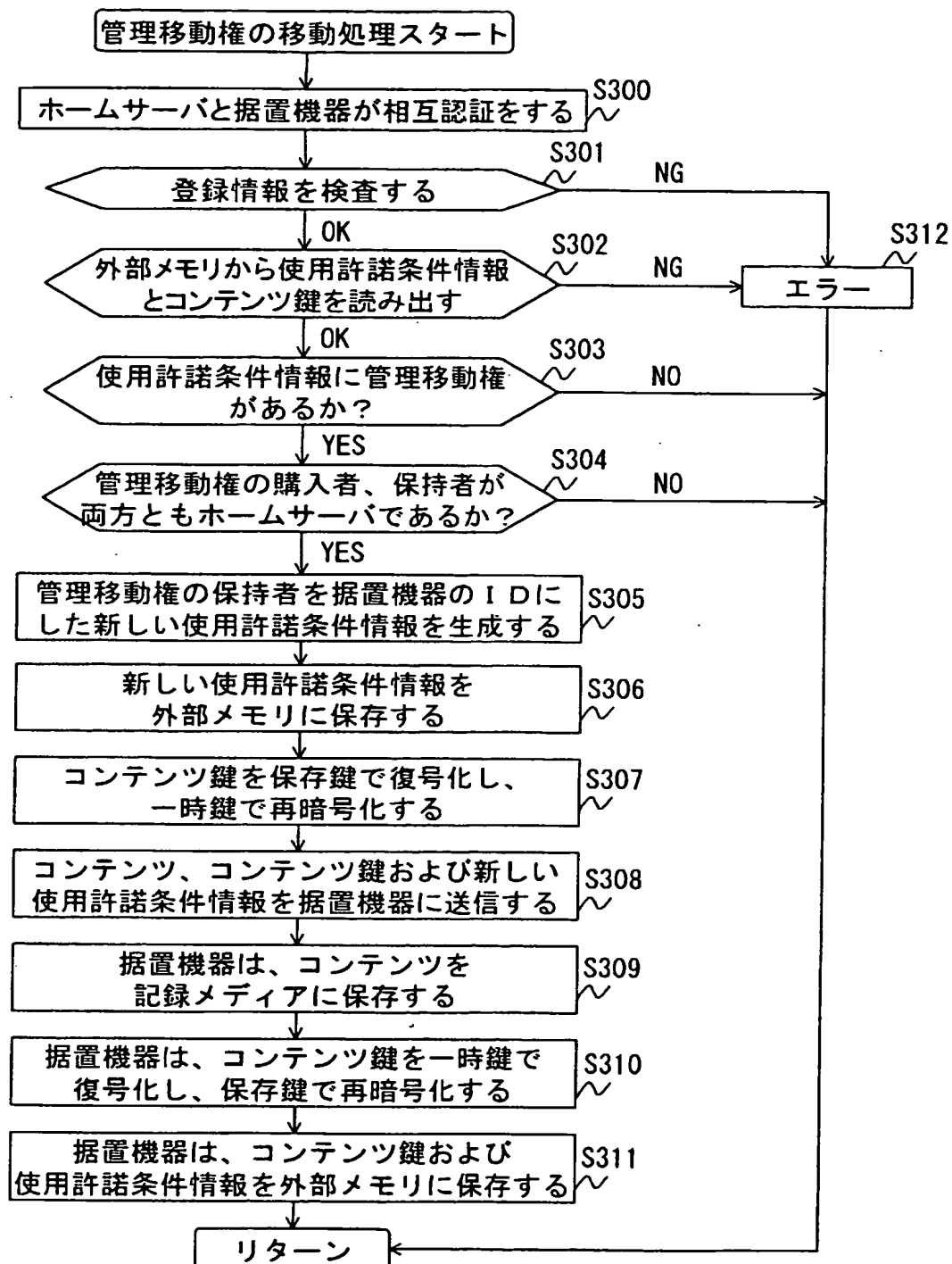


図 8 2

**THIS PAGE BLANK (USPTO)**

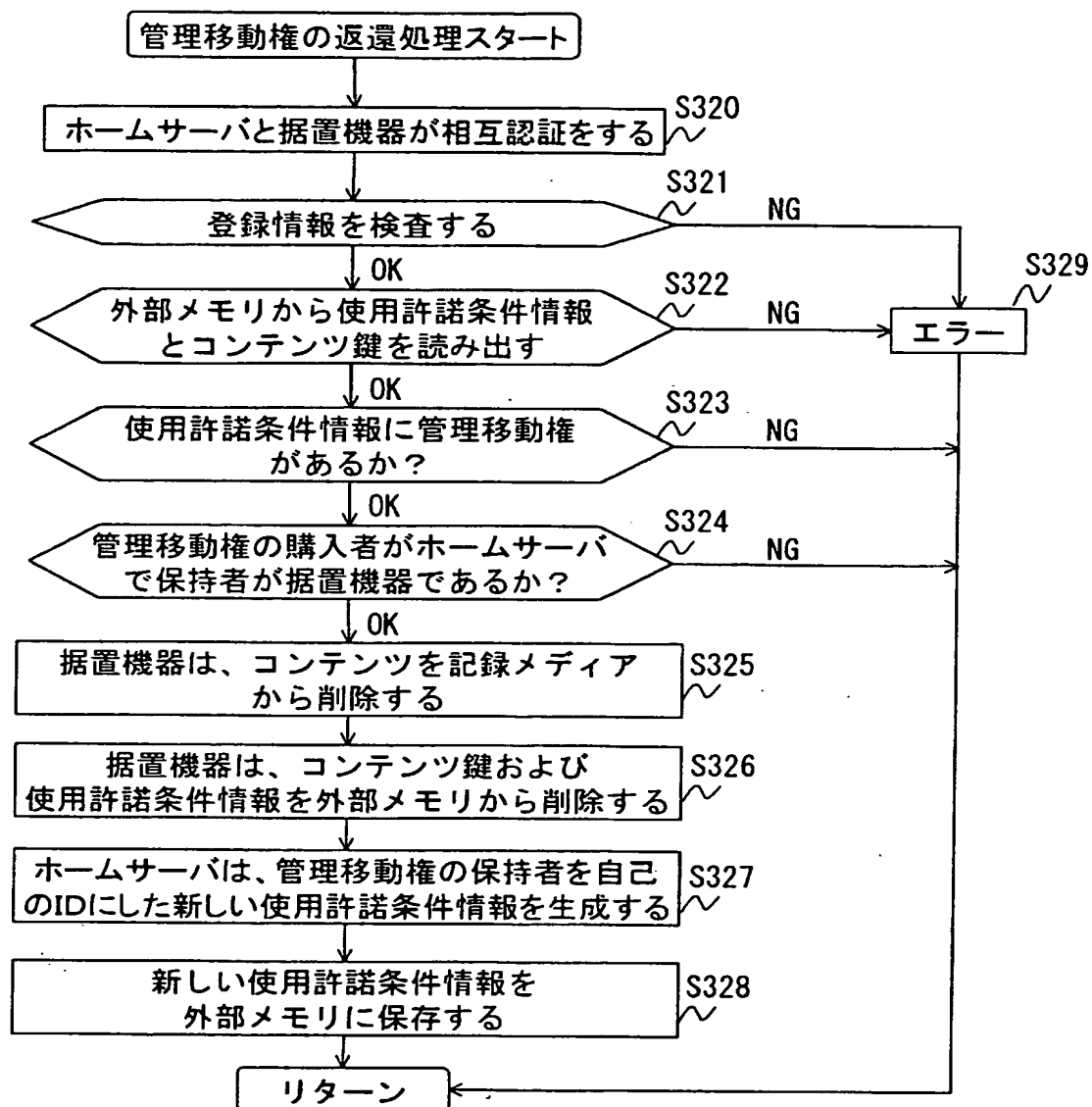
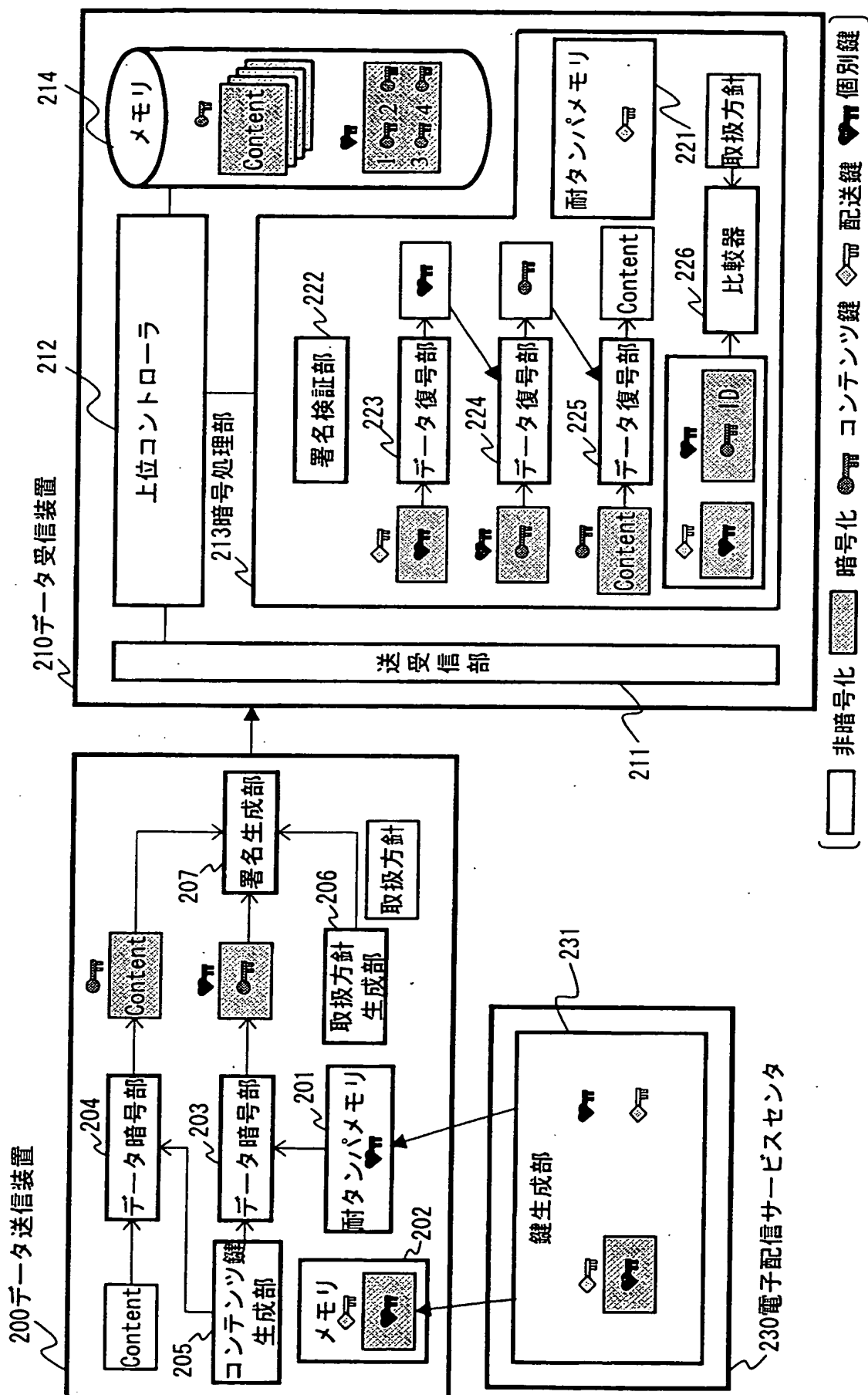



図 8 3

**THIS PAGE BLANK (USPTO)**



48 

**THIS PAGE BLANK (USPTO)**



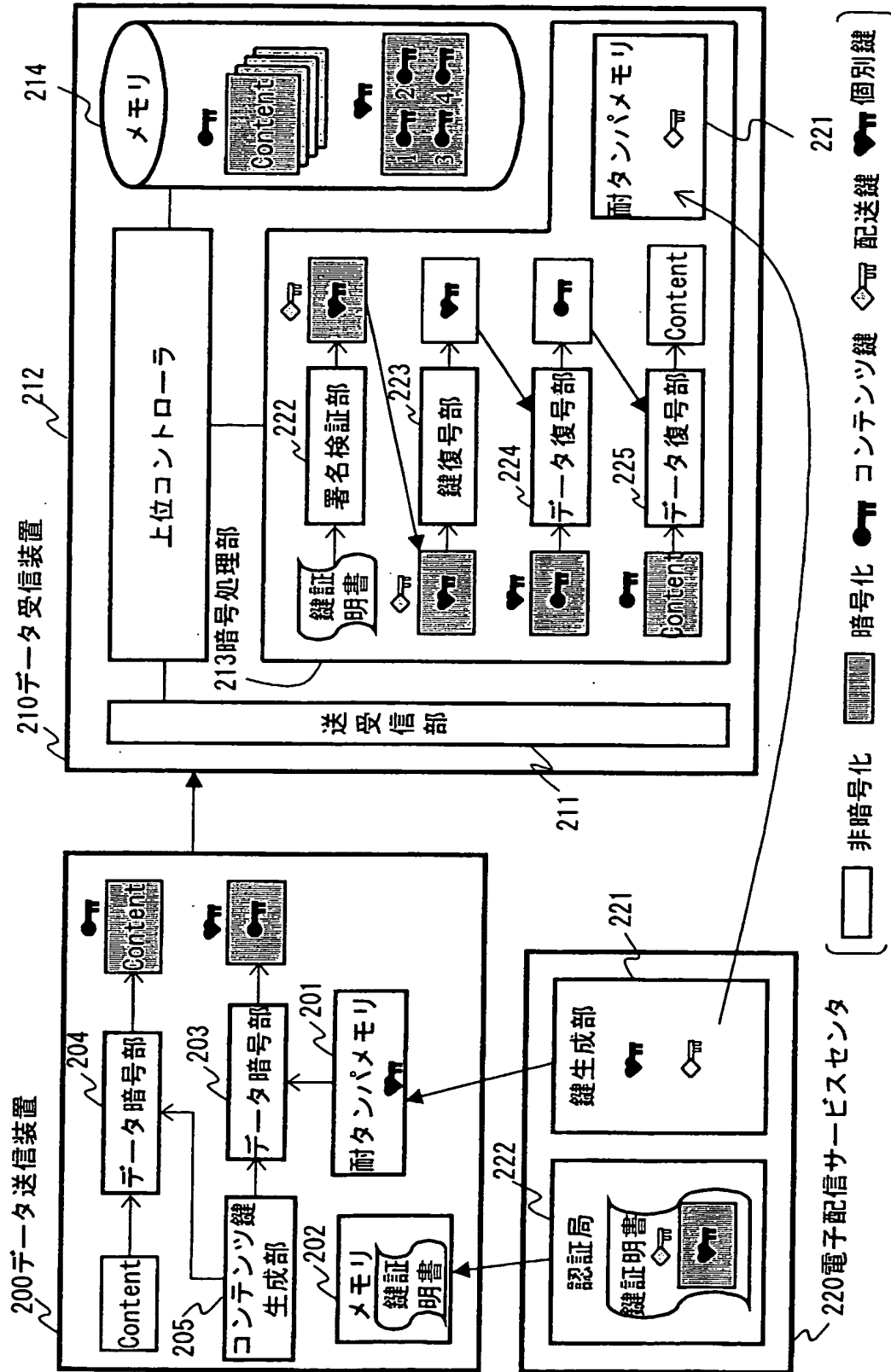


図 8 5

**THIS PAGE BLANK (USPTO)**

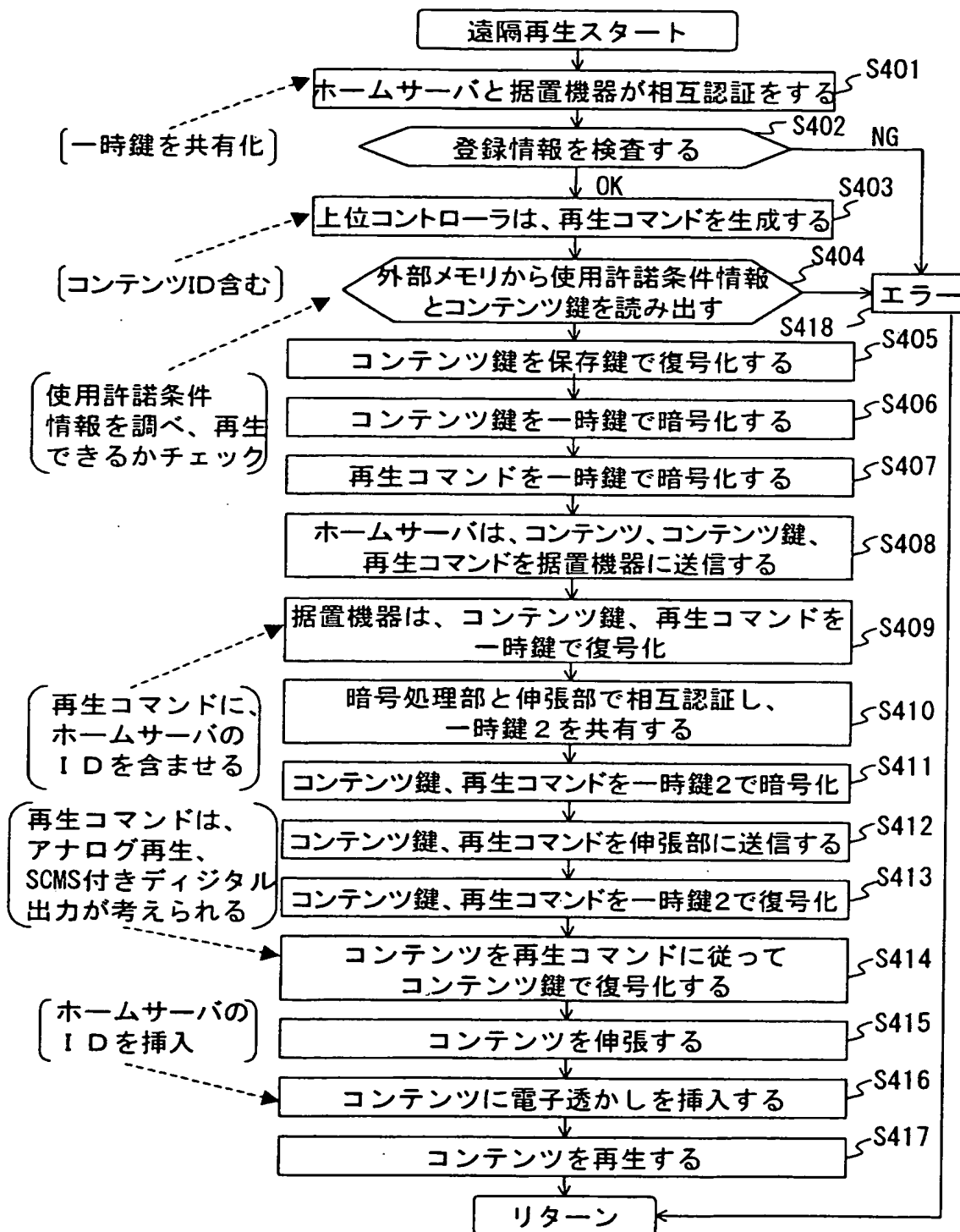


図 8 6

**THIS PAGE BLANK (USPTO)**

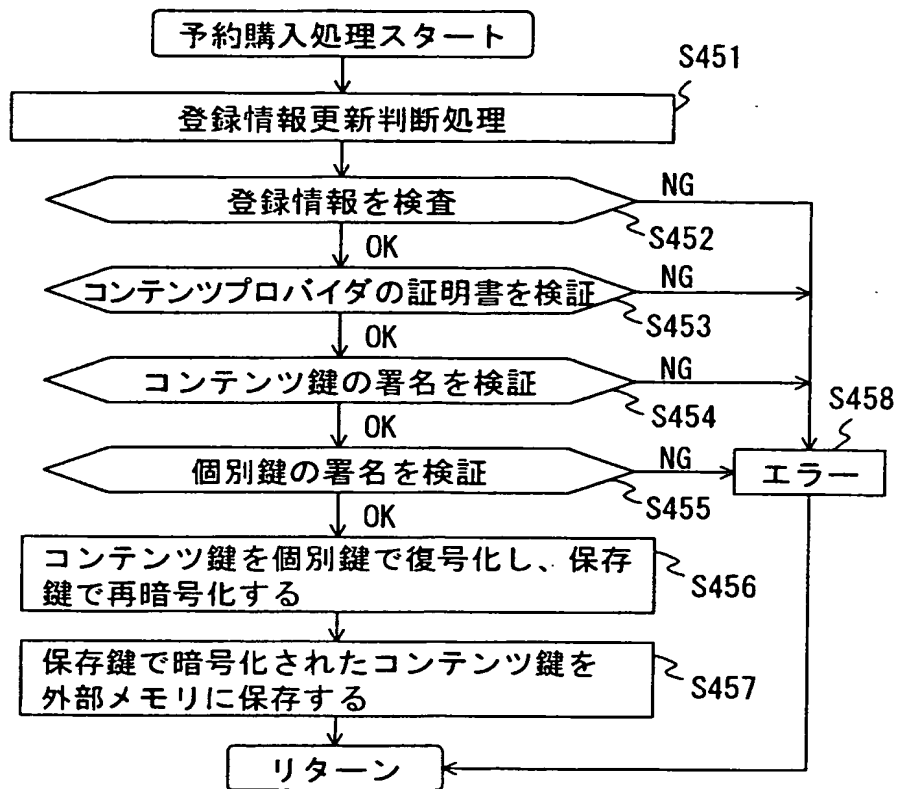


図 8 7

**THIS PAGE BLANK (USPTO)**

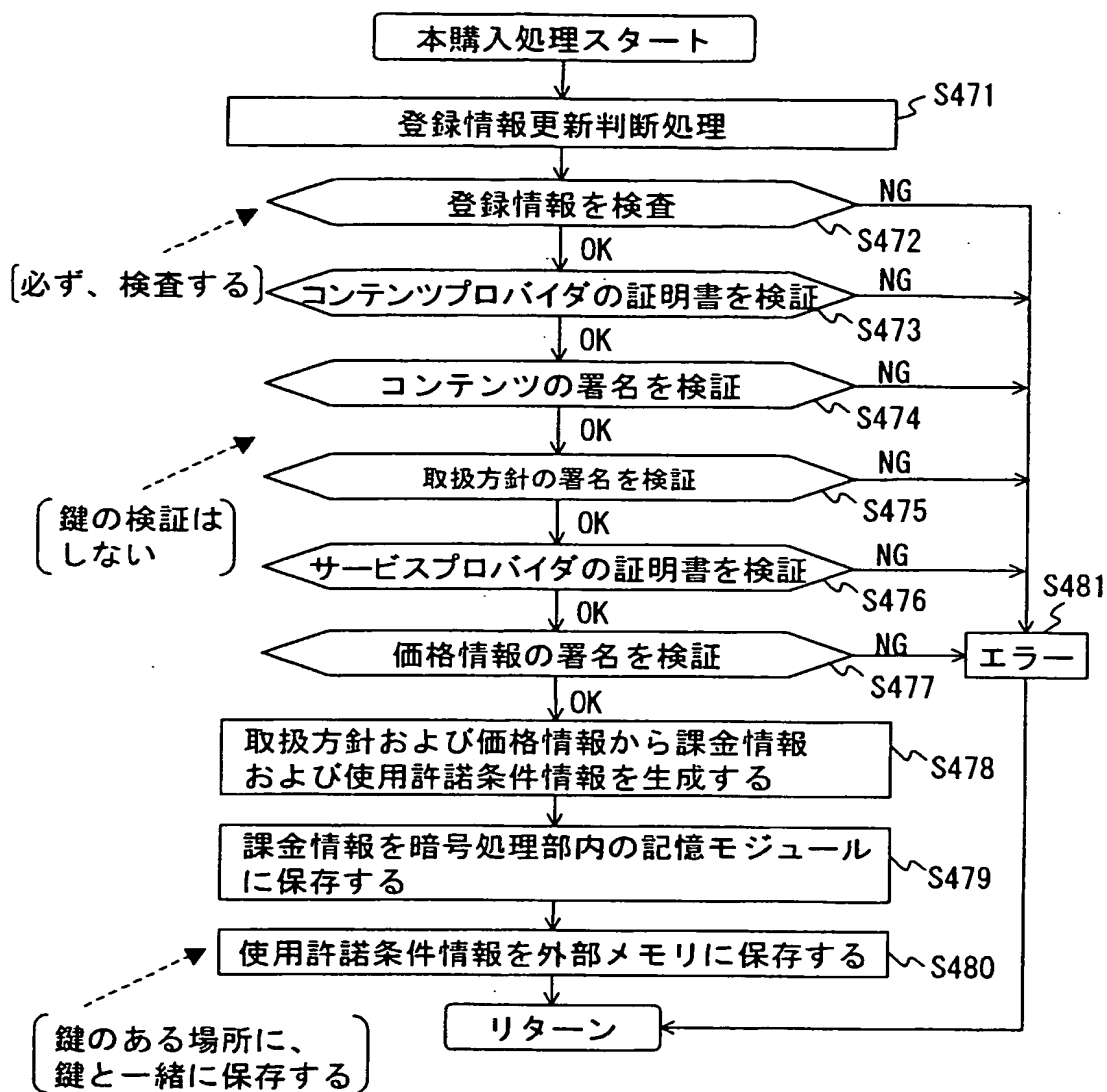


図 8 8

**THIS PAGE BLANK (USPTO)**



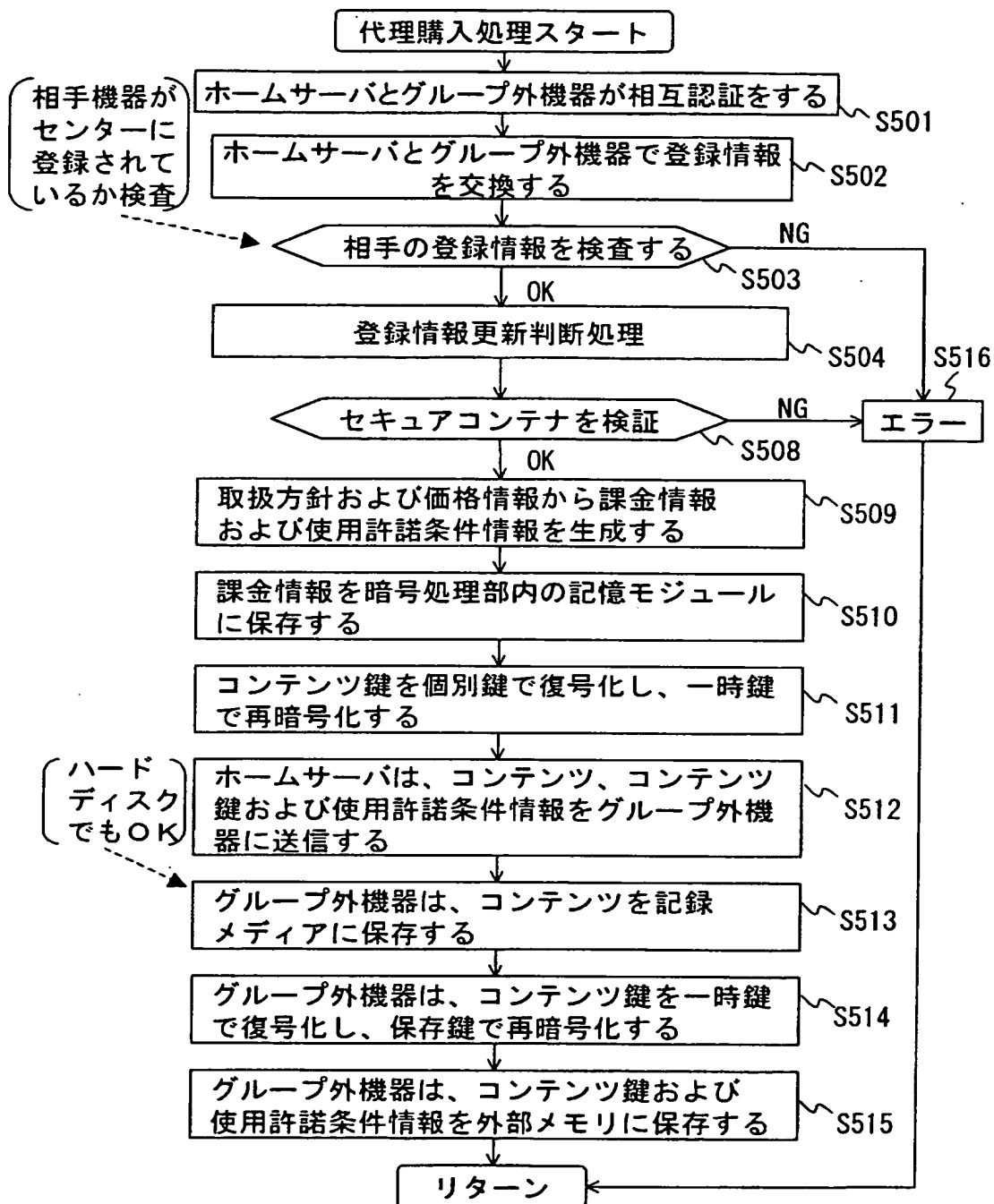


図 89

**THIS PAGE BLANK (USPTO)**

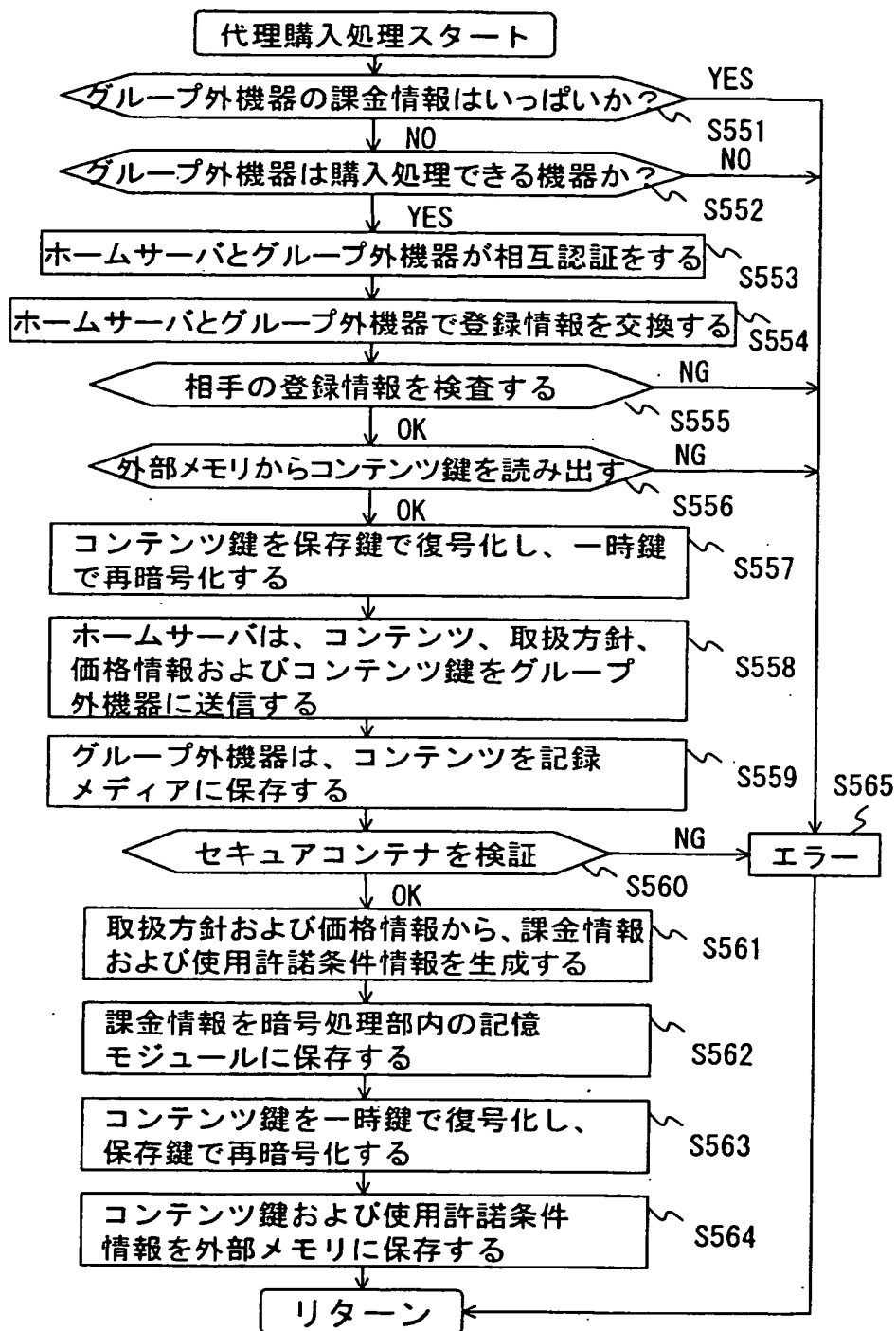


図 90

**THIS PAGE BLANK (USPTO)**

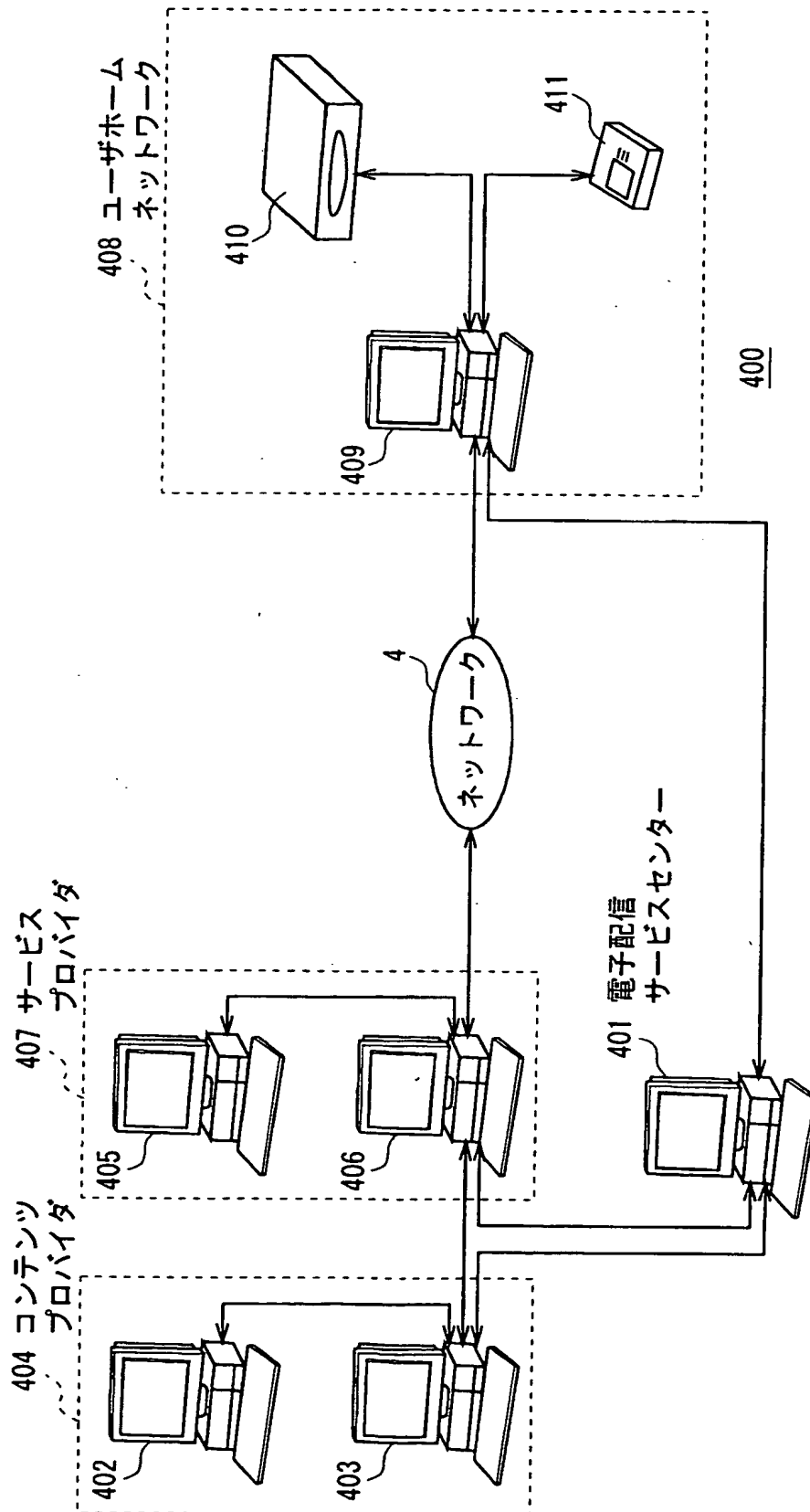


図 91

**THIS PAGE BLANK (USPTO)**

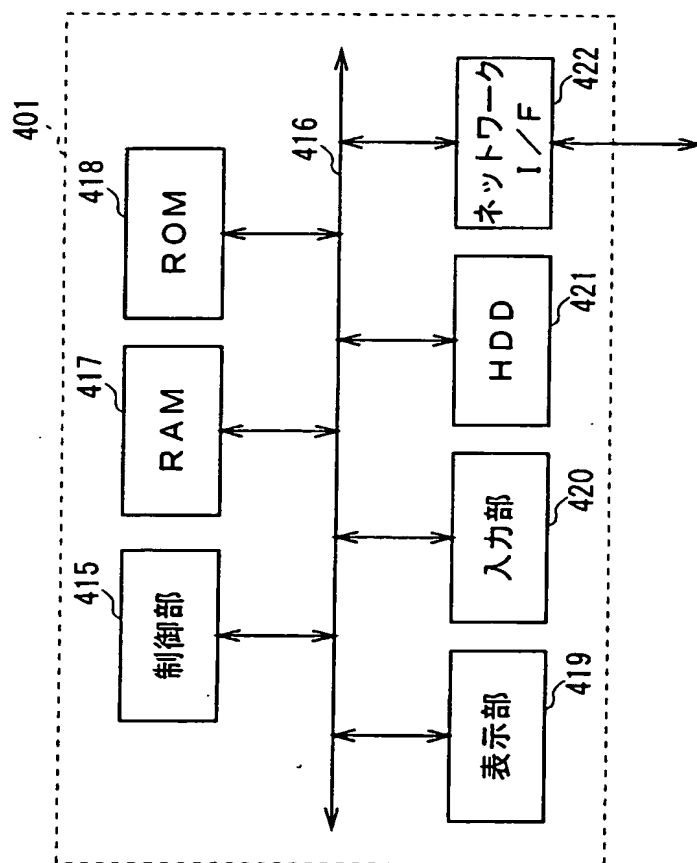


図 9 2

**THIS PAGE BLANK (USPTO)**



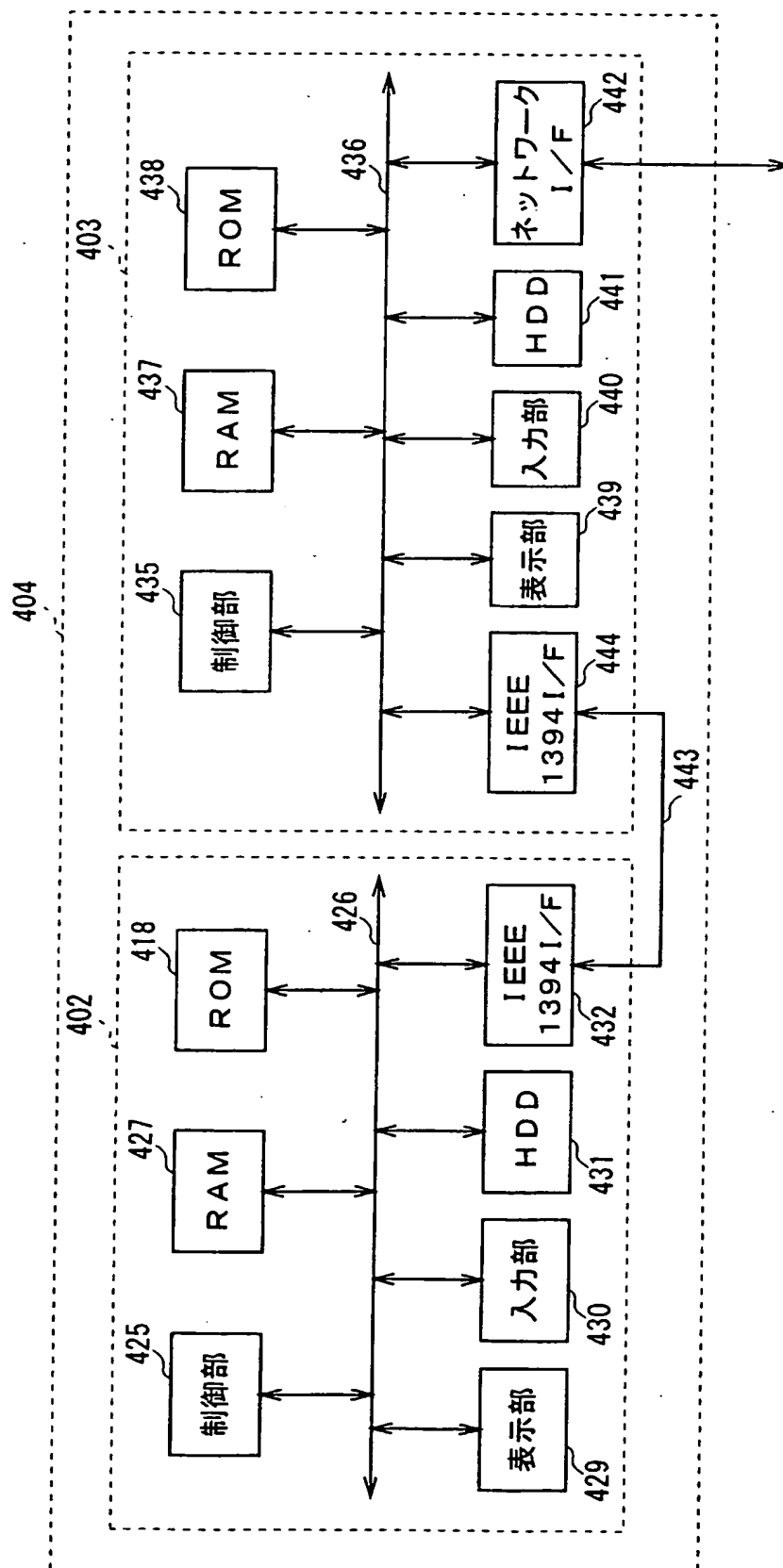


図 93

**THIS PAGE BLANK (USPTO)**

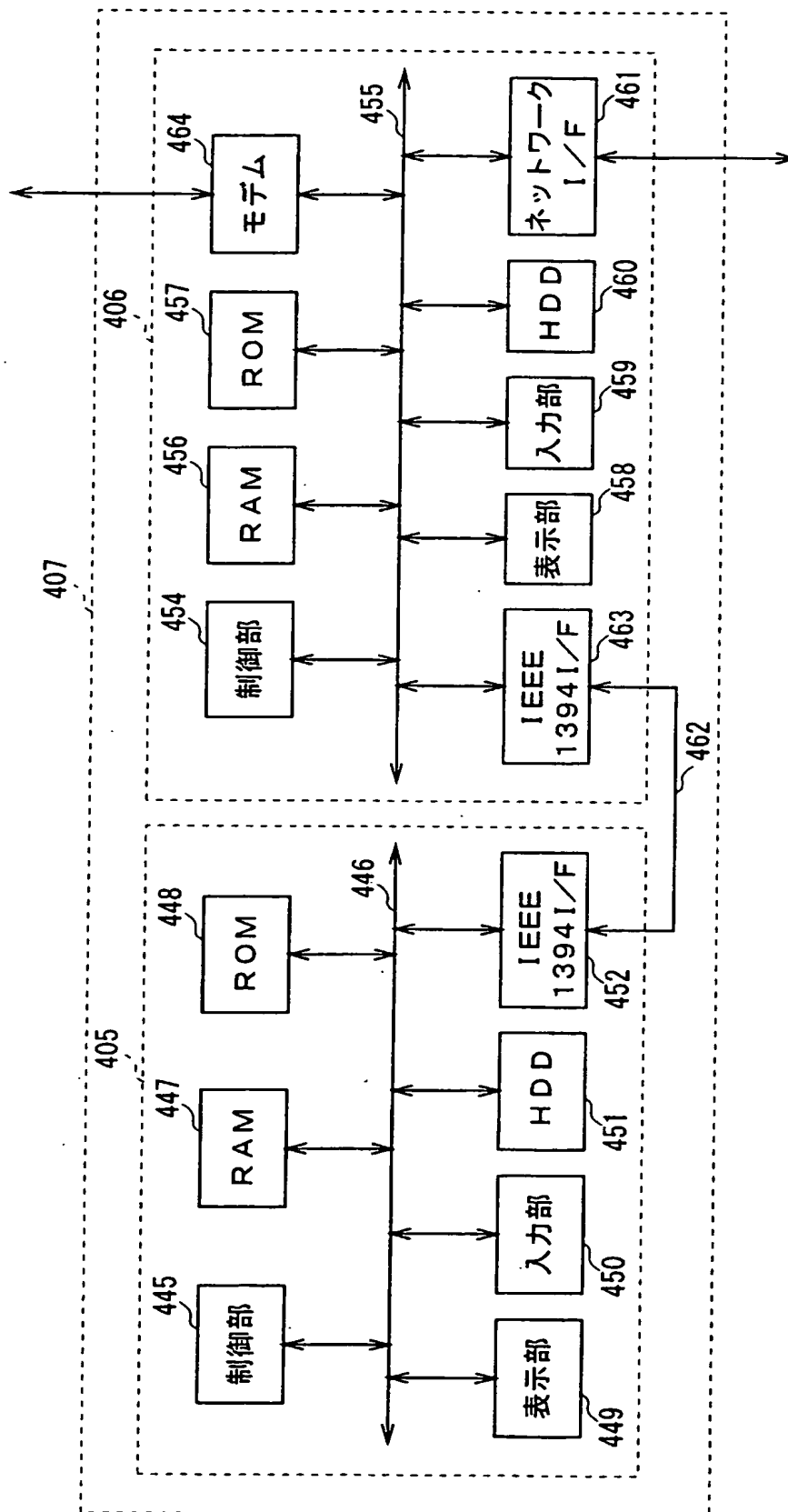


図 9 4

**THIS PAGE BLANK (USPTO)**

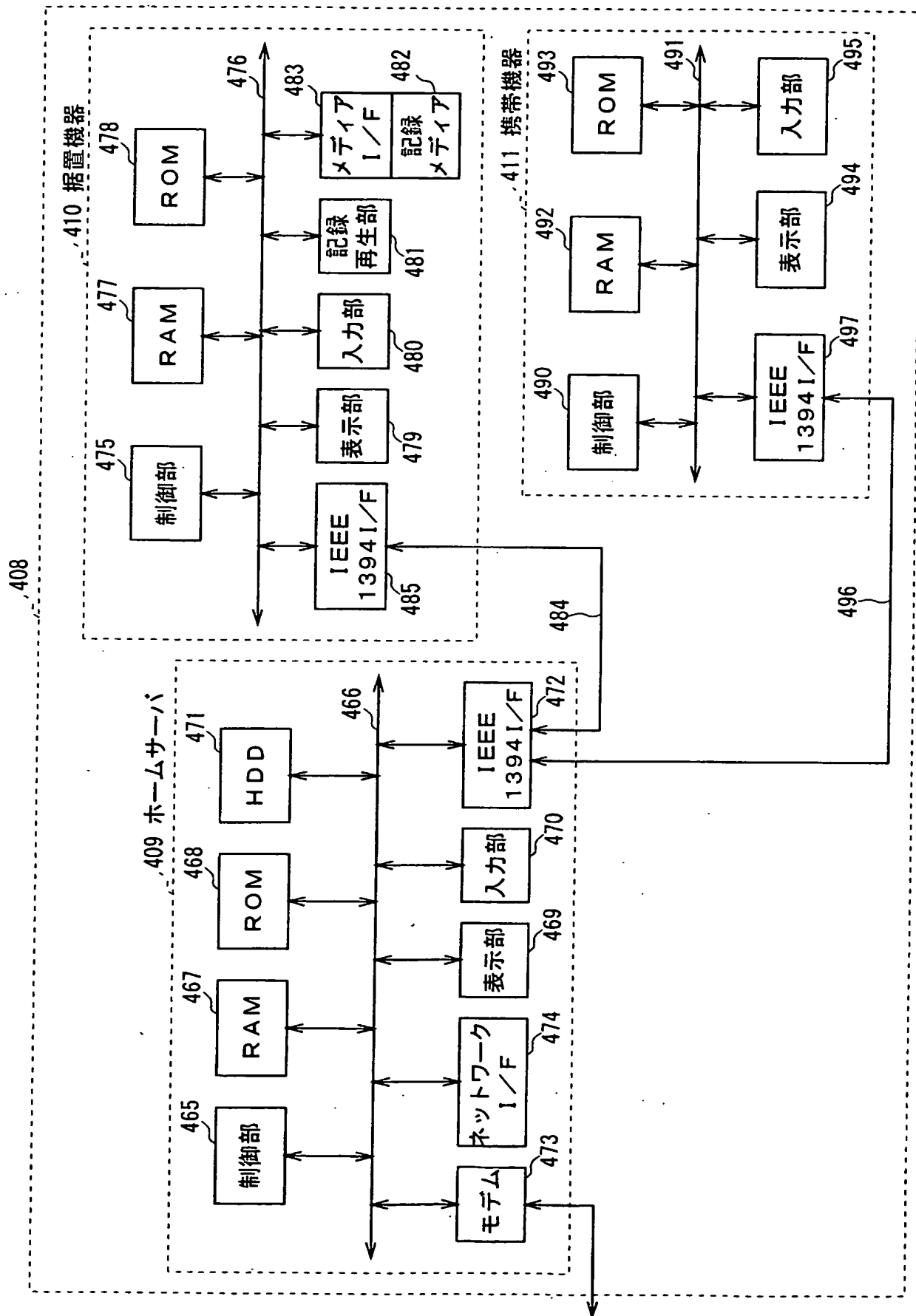


図 95

**THIS PAGE BLANK (USPTO)**

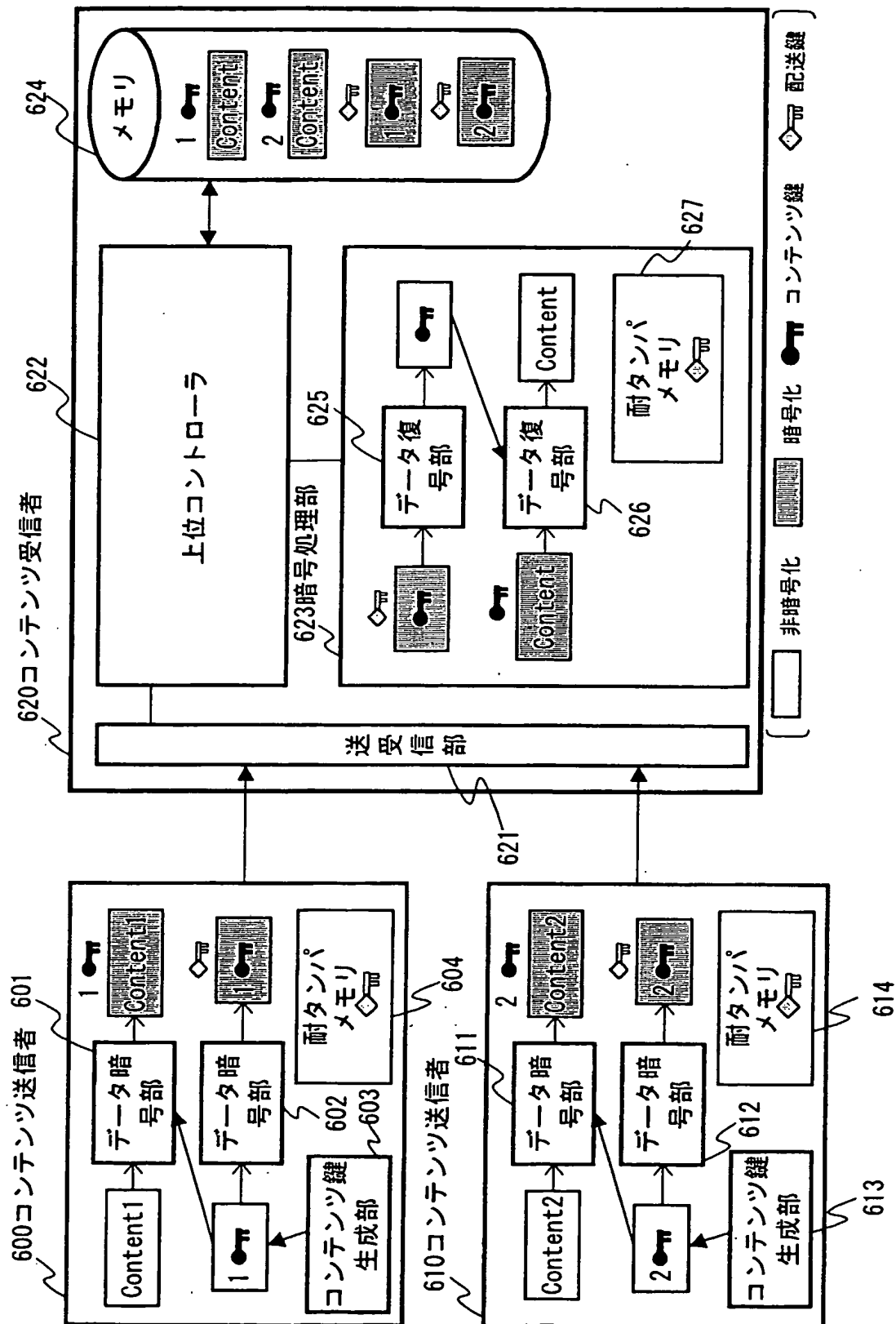


図 9 6

**THIS PAGE BLANK (USPTO)**



## 符 号 の 説 明

1、401……電子配信サービスセンタ、2、404……コンテンツプロバイダ、3、407……サービスプロバイダ、4……ネットワーク、5、408……ユーザホームネットワーク、10、400……電子音楽配信システム、11……サービスプロバイダ管理部、12……コンテンツプロバイダ管理部、13……著作権管理部、14……鍵サーバ、15……経歴データ管理部、16……利益分配部、17……相互認証部、18……ユーザ管理部、19……課金請求部、20……出納部、21……監査部、22……認証局、23……コンテンツサーバ、24……コンテンツオーサリング部、31……コンテンツサーバ、32……電子透かし付加部、34……コンテンツ暗号部、35……コンテンツ鍵生成部、36……コンテンツ鍵暗号部、37……取扱方針生成部、38……署名生成部、39……相互認証部、41……コンテンツサーバ、42……証明書検証部、43……署名検証部、44……値付け部、45……署名生成部、46……相互認証部、51、409……ホームサーバ、52、410……据置機器、53、411……携帯機器、62、72、82……上位コントローラ、65、73、83……暗号処理部、66、74、84……伸張部、67、79、85……外部メモリ、120……電子配信専用記録メディア、402、405……サーバ用パーソナルコンピュータ、403、406……信号処理用パーソナルコンピュータ。

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05742

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the application are separated into six groups: inventions of claims 1-68, those of claims 69-94, those of claims 95-117, those of claims 118-147, those of claims 148-170, and those of claims 171-212.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05742

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP, 684721, B1 (Sony Corporation), 29 November, 1995 (29.11.95), Full text & JP, 8-46948, A & CA, 2149989, A & BR, 9502531, A & CN, 1126339, A & US, 5699426, A & JP, 2000-217071, A & JP, 2000-217072, A & JP, 2000-228662, A	171-212
A	WO, 99/09718, A1 (Sony Corporation), 25 February, 1999 (25.02.99), Full text & AU, 9886472, A & EP, 933901, A1 & CN, 1242899, A	171-212
A	WO, 97/14249, A1 (Matsushita Electric Ind. Co., Ltd.), 17 April, 1997 (17.04.97), Full text & JP, 10-79174, A & EP, 789361, A2 & EP, 800312, A1 & US, 6047103, A & KR, 98700776, A & KR, 98004075, A & TW, 34657, A	171-212

A. 発明の属する分野の分類 (国際特許分類 (IPC))		
Int. Cl' G06F15/00, G06F17/60, H04L9/08, G10K15/02		
B. 調査を行った分野		
調査を行った最小限資料 (国際特許分類 (IPC))		
Int. Cl' G06F15/00, G06F17/60, H04L9/08, G10K15/02, H04N7/16		
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926-1996年 日本国公開実用新案公報 1971-2000年 日本国実用新案登録公報 1996-2000年 日本国登録実用新案公報 1994-2000年		
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)		
WPI, JICST科学技術文献データベース contents, distribution, SuperDistribution, 有料放送		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP, 11-85504, A (三菱電機株式会社) 30. 3月.1999(30.03.99), 第12欄第26-31行 (ファミリーなし)	3-7, 10-24, 26-42, 44-60, 62-68
A		1, 2, 8, 9, 25, 43, 61
Y	JP, 10-161937, A (株式会社東芝) 19. 6月.1998(19.06.98), 第17欄第1-19行 (ファミリーなし)	3-7, 10-24, 26-42, 44-60, 62-68
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願		
の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献		
国際調査を完了した日	22. 12. 00	国際調査報告の発送日 16.01.01
国際調査機関の名称及びあて先	特許庁審査官 (権限のある職員)	5M 9364
日本国特許庁 (ISA/JP)	中里 裕正	
郵便番号100-8915	電話番号 03-3581-1101	内線 3599
東京都千代田区霞が関三丁目4番3号		

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A		1, 2, 8, 9, 25, 43, 61
Y	US, 5701343, A (Nippon Telegraph & Telephone Corp.) 23. 12月. 1997 (23. 12. 97), 第9欄第64行-第10欄第14行 & JP, 8-160855, A & JP, 8-160856, A & EP, 715242, A1	6, 7, 13, 14, 22, 23, 31, 40, 41, 49, 58, 59, 67
Y	WO, 96/27155, A2 (Electronic Publishing Resources, Inc.) 6. 9月. 1996 (06. 09. 96), 第389-390, 397-407頁 & JP, 10-512074, A & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A & US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	16, 34, 52, 118, 119, 121, 122, 124, 128, 132, 136, 140, 144
A		120, 123, 125- 127, 129-131, 133-135, 137- 139, 141-143, 145-147
A	US, 5673316, A (International Business Machines Corporation) 29. 6月. 1996 (29. 06. 96), 第5欄第14-43行 & JP, 10-40100, A & EP, 798892, A2 & KR, 187876, B1	1-68
A	FleaMarket方式による情報流通、マルチメディア通信と分散処理ワ ークショップ論文集 Vol. 95 No. 2, 情報処理学会, 25. 10月. 1995 (25. 10. 95), 3. 2. 1カプセルの構造	1-68
X	JP, 4-297145, A (株式会社東芝) 21. 10月. 1992 (21. 10. 92), 特許請求の範囲, 図2 (ファミリーなし)	69-71, 75, 79, 83, 87, 91
X	放送における情報セキュリティ技術, 電子情報通信学会研究報告, Vol. 89 No. 356 (ISEC89-35), 電子情報通信学会, 18. 12月. 1989 (18. 12. 89), 4. システム内の秘密要素と安全性, 図3	69-72, 75, 76, 79, 80, 83, 84, 87, 88, 91, 92, 95-98, 101, 104, 105, 108, 109, 111, 112, 115
Y		73, 74, 77, 78, 81, 82, 85, 86, 89, 90, 93, 94, 99, 100, 102, 103, 106, 107, 109, 110, 113,

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05742

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08, G10K15/02

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F15/00, G06F17/60, H04L9/08, G10K15/02, H04N7/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2000
Kokai Jitsuyo Shinan Koho	1971-2000	Toroku Jitsuyo Shinan Koho	1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, JICST SCIENCE TECHNOLOGY DOCUMENT DATABASE contents, distribution, Super Distribution, payable broadcast (in Japanese)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 11-85504, A (Mitsubishi Electric Corporation), 30 March, 1999 (30.03.99), Column 12, lines 26 to 31 (Family: none)	3-7, 10-24, 26-4 2, 44-60, 62-68
A		1, 2, 8, 9, 25, 43, 61
Y	JP, 10-161937, A (Toshiba Corporation), 19 June, 1998 (19.06.98), Column 17, lines 1 to 19 (Family: none)	3-7, 10-24, 26-4 2, 44-60, 62-68
A		1, 2, 8, 9, 25, 43, 61
Y	US, 5701343, A (Nippon Telegraph & Telephone Corp.), 23 December, 1997 (23.12.97), Column 9, line 64 to Column 10, line 14 & JP, 8-160855, A & JP, 8-160856, A & EP, 715242, A1	6, 7, 13, 14, 22, 23, 31, 40, 41, 49, 58, 59, 67
Y	WO, 96/27155, A2 (Electronic Publishing Resources, Inc.), 06 September, 1996 (06.09.96), pages 389 to 390, 397 to 407 & JP, 10-512074, A & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A	16, 34, 52, 118, 119, 121, 122, 124, 128, 132, 136, 140, 144

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
22 December, 2000 (22.12.00)Date of mailing of the international search report  
16 January, 2001 (16.01.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/05742

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	& US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	120,123,125- 127,129-131, 133-135,137- 139,141-143, 145-147
A	US, 5673316, A (International Business Machines Corporation), 29 June, 1996 (29.06.96), Column 5, lines 14 to 43 & JP, 10-40100, A & EP, 798892, A2 & KR, 187876, B1	1-68
A	Flea Market Houshiki ni yoru Jouhou Ryutsu, Multi media Tsushin to Bunsan Shori Workshop Ronbunshu, Vol. 95, No.2, Information Processing Society of Japan (IPSJ), 25 October, 1995 (25.10.95), 3.2.1 "Capsule no Kouzou"	1-68
X	JP, 4-297145, A (Toshiba Corporation), 21 October, 1992 (21.10.92), Claims; Fig. 2 (Family: none)	69-71,75,79, 83,87,91
X	Housou ni okeru Johou Security Gijutsu, Technical research report, the Institute of Electronics, Information and Communication Engineers, Vol.89, No.356 (ISEC89-35), the Institute of Electronics, Information and Communication Engineers, 18 December, 1989 (18.12.89), 4. "System nai no Himitsu Youso to Anzensei"; Fig. 3	69-72,75,76, 79,80,83,84, 87,88,91,92, 95-98,101, 104,105,108,10 9,111,112,115
Y		73,74,77,78, 81,82,85,86, 89,90,93,94, 99,100,102, 103,106,107, 109,110,113, 114,116,117
		148-170
A		
Y	JP, 7-154770, A (NEC Corporation), 16 June, 1995 (16.06.95), Full text (Family: none)	73,74,77,78, 81,82,85,86, 89,90,93,94
A		148-170
Y	EP, 542345, B1 (N. V. Phillips'Gloeilampfabrieken), 04 November, 1992 (04.11.92), Column 12, lines 7 to 21 & JP, 6-180974, A & US, 5313524, A & TW, 798892, A2 & KR, 187876, B1 & DE, 69220180, E1	118,119,121, 122,124,128, 132,136,140, 144
A		120,123,125- 127,129-131, 133-135,137- 139,141-143, 145-147



## 第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (C T 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

この出願の発明は、請求の範囲1-68/69-94/95-117/118-147/148-170/171-212の6群の発明に区分される。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。  
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A		114, 116, 117
Y	JP, 7-154770, A (日本電気株式会社) 16. 6月. 1995 (16. 06. 95), 全頁を参照 (ファミリーなし)	148-170
A		73, 74, 77, 78, 81, 82, 85, 86, 89, 90, 93, 94
Y	EP, 542345, B1 (N.V. Phillips' Gloeilampfabrieken) 04. 11月. 1992 (04. 11. 92), 第12欄第7-21行 & JP, 6-180974, A & US, 5313524, A & TW, 798892, A2 & KR, 187876, B1 & DE, 69220180, E1	148-170
A		118, 119, 121, 122, 124, 128, 132, 136, 140, 144
A		120, 123, 125- 127, 129-131, 133-135, 137- 139, 141-143, 145-147
A	EP, 684721, B1 (ソニー株式会社) 29. 11月. 1995 (29. 11. 95), 全頁を参照 & JP, 8-46948, A & CA, 2149989, A & BR, 9502531, A & CN, 1126339, A & US, 5699426, A & JP, 2000-217071, A & JP, 2000-217072, A & JP, 2000-228662, A	171-212
A	WO, 99/09718, A1 (ソニー株式会社) 25. 2月. 1999 (25. 02. 99), 全頁を参照 & AU, 9886472, A & EP, 933901, A1 & CN, 1242899, A	171-212
A	WO, 97/14249, A1 (松下電器産業株式会社) 17. 4月. 1997 (17. 04. 97), 全頁を参照 & JP, 10-79174, A & EP, 789361, A2 & EP, 800312, A1 & US, 6047103, A & KR, 98700776, A & KR, 98004075, A & TW, 34657, A	171-212